



Transportation
Security
Administration

October 30, 2020

3600.1

Case Number: 2020-TSFO-00198

Ashley Gorski
Patrick Toomey
Nathan Freed Wessler
American Civil Liberties Union
Foundation
125 Broad Street, 18th Floor
New York, NY 10004
agorski@aclu.org
nspfoia@aclu.org

Dear Ms. Gorski:

This is the Transportation Security Administration's (TSA) fourth interim response to your Freedom of Information Act (FOIA) request dated January 09, 2020, addressed to the TSA FOIA Branch seeking access to "records pertaining to the use of facial recognition technology at airports and at the border by the Department of Homeland Security ('DHS'), U.S. Customs and Border Protection ('CBP'), and the Transportation Security Administration ('TSA')." That request seeks the following records from TSA:

1. All policies, procedures, guidelines, formal or informal guidance, advisories, directives, and memoranda concerning:

- a. The acquisition, processing, retention, or dissemination of data collected or generated through CBP's biometric services and infrastructure, including biometric templates;*
- b. Access by airlines, airports, cruise lines, seaports, commercial vendors, other countries, or other U.S. federal, state, or local authorities to data collected or generated through CBP's biometric services and infrastructure, including biometric templates;*
- c. Retention or dissemination by airlines, airports, cruise lines, seaports, commercial vendors, other countries, or other U.S. federal, state, or local authorities of data collected or generated through CBP's biometric services and infrastructure, including biometric templates.*

2. All final evaluations, tests, audits, analyses, studies, or assessments by the DHS Science and Technology Directorate, DHS Office of Biometric Identity Management, or the National Institute of Standards and Technology related to (i) the performance of algorithms in matching facial photographs, and/or (ii) the performance of facial recognition technologies developed by vendors. This request encompasses records concerning whether the algorithms or technologies perform differently based on flight route or an individual's race, ethnicity, skin pigmentation, gender, age, and/or country of origin.

3. All records, excluding informal email correspondence, concerning future interoperability between the TSA's biometric capabilities and "mission partner systems," including CBP and DHS Office of Biometric Identity Management systems.

4. All policies, procedures, guidelines, formal or informal guidance, advisories, directives, and memoranda concerning requests by other federal agencies (including but not limited to the FBI, the DEA, the CIA, and the U.S. Marshals) for TSA assistance in locating or identifying individuals, and all requests by federal agencies for TSA cooperation in designing systems to facilitate information-sharing. [Note that we understand that in May 2020 the ACLU agreed to rephrase this request as follows: 'All policies, procedures and guidelines concerning requests by other federal agencies (including but not limited to the FBI, the DEA, the CIA, and the U.S. Marshals) for TSA assistance in locating or identifying individuals, and all requests by federal agencies for TSA cooperation in designing systems to facilitate biometric information-sharing.']

5. All records, excluding informal email correspondence, concerning the TSA's plans to "complement the capabilities" of Credential Authentication Technology through the implementation of TVS or facial recognition technology with respect to domestic travelers.

6. All records, excluding informal email correspondence, concerning whether implementation of biometric technologies would result in operational efficiencies, including whether, at certain airport facilities, "the throughput of the checkpoint may be largely unaffected" by biometric technology because "a faster [travel document checker] process would merely shift traveler volume from the queue into the screening lane."

The processing of TSA's fourth interim response identified certain records that will be released to you. Portions not released are being withheld pursuant to the Freedom of Information Act, 5 U.S.C. § 552. Please refer to the Applicable Exemptions list at the end of this letter that identifies the authority for withholding the exempt records by marking the block next to the applicable exemptions. An additional enclosure with this letter explains these exemptions in more detail.

For this fourth interim response, the TSA FOIA Branch reviewed 371 pages to include the 116 pages that were under review by the Sensitive Security Information Program office. Of the 371 pages, we have released in full 54 pages, released in part (with redactions) 14 pages, withheld in full 64 pages, and identified 178 pages as non-responsive. Additionally, we have sent 61 pages to CBP for consultation. We await input on the 33 pages sent to DHS for consultation from the last interim response.

The rules and regulations of the Transportation Security Administration applicable to Freedom of Information Act requests are contained in the Code of Federal Regulations, Title 6, Part 5. They are published in the Federal Register and are available for inspection by the public.

Administrative Appeal

Because TSA's response to this request is currently the subject of litigation, the administrative appeal rights normally associated with a FOIA request response are not being provided.

If you have any questions pertaining to your request, please contact AUSA Jennifer Jude at jennifer.jude@usdoj.gov.

Sincerely,



Teri M. Miller
FOIA Officer

Summary:

Number of Pages Released in Part or in Full: 68

Number of Pages Withheld in Full: 64

**APPLICABLE EXEMPTIONS
FREEDOM OF INFORMATION ACT AND/OR PRIVACY ACT**

Freedom of Information Act (5 U.S.C. 552)

(b)(1) (b)(2) (b)(3) (b)(4) (b)(5) (b)(6)

(b)(7)(A) (b)(7)(B) (b)(7)(C) (b)(7)(D) (b)(7)(E) (b)(7)(F)

Enclosures

FREEDOM OF INFORMATION ACT
SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552

Transportation Security Administration (TSA) FOIA Branch applies FOIA exemptions to protect:

Exemptions

Exemption (b)(1): Records that contain information that is classified for national security purposes.

Exemption (b)(2): Records that are related solely to the internal personnel rules and practices of an agency.

Exemption (b)(3): Records specifically exempted from disclosure by Title 49 U.S.C. Section 114(r), which exempts from disclosure Sensitive Security Information (SSI) that “would be detrimental to the security of transportation” if disclosed.

Exemption (b)(4): Records that contain trade secrets and commercial or financial information obtained from a person that is privileged or confidential.

Exemption (b)(5): Inter- or intra-agency records that are normally privileged in the civil discovery context. The three most frequently invoked privileges are the deliberative process privilege, the attorney work-product privilege, and the attorney-client privilege:

- Deliberative process privilege – Under the deliberative process privilege, disclosure of these records would injure the quality of future agency decisions by discouraging the open and frank policy discussions between subordinates and superiors.
- Attorney work-product privilege – Records prepared by or at the direction of a TSA attorney.
- Attorney-client privilege – Records of communications between an attorney and his/her client relating to a matter for which the client has sought legal advice, as well as facts divulged by client to attorney and any opinions given by attorney based on these.

Exemption (b)(6): Records that contain identifying information that applies to a particular individual when the disclosure of such information “would constitute a clearly unwarranted invasion of personal privacy.” This requires the balancing of the public’s right to disclosure against the individual’s right to privacy.

Exemption (b)(7)(A): Records or information compiled for law enforcement purposes, but only to the extent that production of such law enforcement records or information...could reasonably be expected to interfere with law enforcement proceedings.

Exemption (b)(7)(C): Records containing law enforcement information when disclosure “could reasonably be expected to constitute an unwarranted invasion of personal privacy” based upon the traditional recognition of strong privacy interests ordinarily appropriated in law enforcement records.

Exemption (b)(7)(E): Records compiled for law enforcement purposes, the release of which would disclose techniques and/or procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law.

Exemption (b)(7)(F): Records containing law enforcement information about a person, in that disclosure of information about him or her could reasonably be expected to endanger his or her life or physical safety.

PRIVACY ACT
SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552a

Transportation Security Administration (TSA) FOIA Branch applies Privacy Act exemptions to protect:

Exemptions

Exemption (d)(5): Information compiled in reasonable anticipation of civil action or proceeding; self-executing exemption.

Exemption (j)(2): Principal function criminal law enforcement agency records compiled during course of criminal law enforcement proceeding.

Exemption (k)(1): classified information under an Executive Order in the interest of national defense or foreign policy.

Exemption (k)(2): Non-criminal law enforcement records; criminal law enforcement records compiled by non-principal function criminal law enforcement agency; coverage is less broad where individual has been denied a right, privilege, or benefit as result of information sought.

Exemption (k)(5): Investigatory material used only to determine suitability, eligibility, or qualifications for federal civilian employment or access to classified information when the material comes from confidential sources.

Exemption (k)(6): Testing or examination material used to determine appointment or promotion of federal employees when disclosure would compromise the objectivity or fairness of the process.

Page 01

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 02

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 03

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 04

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

~~_____~~

Page 05

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

~~_____~~

Page 06

Withheld pursuant to exemption

(b)(5) ; (b)(3):49 U.S.C. § 114(r)

of the Freedom of Information and Privacy Act

Page 07

Withheld pursuant to exemption

(b)(5) ; (b)(3):49 U.S.C. § 114(r)

of the Freedom of Information and Privacy Act

Page 08

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 09

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

~~_____~~

Page 10

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 11

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 12

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

~~_____~~

Page 13

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 14

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 15

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 16

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 17

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 18

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 19

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 20

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 21

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 22

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 23

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Page 24

Withheld pursuant to exemption

(b)(5)

of the Freedom of Information and Privacy Act

Section I.B.1.b. of Emergency Amendment 1546-12-07K requires foreign air carriers to compare each passenger's travel document with his or her valid passport or valid government-issued photo ID when the passenger tenders checked baggage to the foreign air carrier within a U.S. airport facility.

On June 7, 2018, DALA submitted a request for an amendment to use CBP's Traveler Verification Service (TVS) facial recognition system as a biometric means of passenger identity verification in lieu of an aircraft operator or authorized representative performing a visual comparison. The TVS system operates from a network of cameras at the bag drop and matches the passenger's image against the stored image in CBP's photo gallery compiled from passport and visa information. In a joint biometric partnership between the Transportation Security Administration (TSA) and CBP, the TVS system was successfully piloted at John F. Kennedy International Airport and Boston Logan International Airport and is currently undergoing testing at Los Angeles International Airport.

Discussion

DALA is proposing to operate the TVS system as a proof of concept in Terminal F, their international departure terminal, at ATL. The system works by creating an active gallery of images for those individuals departing ATL that day based on the aircraft operator's Advance Passenger Information System submittals. When a passenger uses the TVS system, their image is photographed and matched against the stored photo gallery created on the CBP platform. Upon confirmation that a match exists, CBP will send a confirmation to DALA's bag drop system that the passenger is considered verified. The aircraft operator will then accept the checked baggage from the passenger. The aircraft operator must continue to comply with all Secure Flight procedures, including Verifying Identity Document procedures when necessary, and ensure any passenger with a returned "Inhibit" status from Secure Flight is prevented from using the biometric bag drop. (b)(3):49 U.S.C. § 114(r)

(b)(3):49 U.S.C. § 114(r) as prescribed in their AOSSP.

DALA provided a draft test plan for the biometric bag drop for TSA's Requirements and Capabilities Analysis (RCA) office to review and approve per the AOSSP amendment review process. DALA is testing the TVS system operating in parallel with a manual ID check. RCA reviewed the test data created to date and deemed it acceptable. DALA has been providing TSA with emerging results since the testing began on October 15, 2018. Based on TSA's current analysis of the provided data, TVS performance at bag drop preliminarily satisfies the match requirements RCA has previously communicated to DALA. These requirements include:

- True Match Rate (O: 97 percent, T: 90 percent)
- False Match Rate / False Positive Identification Rate: < 0.1 percent

We anticipate confirmation of these preliminary results at the conclusion of the testing period on December 6, 2018. Given the data DALA produced to date, we recommend issuance of the amendment to allow DALA to implement an official proof of concept beginning December 1, 2018.

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be released to persons without a "need to know" as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

~~SENSITIVE SECURITY INFORMATION~~

2. The use of the TVS system, for purposes of providing services to the foreign air carrier in connection with this proof of concept, meets or exceeds the information security standards specified and approved by TSA.
 3. The TVS matching thresholds meet or exceed the following:
 - a) True Match Rate of greater than or equal to 97 percent and;
 - b) False Match Rate/False Positive Identification Rate (FPIR) of less than or equal to 0.1 percent and;
 - c) False Non Match Rate (FNMR)/False Negative Identification Rate (FNIR) of less than or equal to 3 percent.
- B. The foreign air carrier's assigned International Industry Representative (IIR) and ATL's Federal Security Director (FSD) or designee must be immediately notified in the event of program information being misplaced or compromised during collection, storage, transmission, or disposal.
- C. Passenger Biometric Bag Drop
1. The foreign air carrier must comply with the following procedures in lieu of those contained in EA 1546-12-07 Series, Section I.B.1.b., only when accepting checked baggage of passengers using valid government issued passports or visas verified by the TVS facial recognition system.
 2. Ensure that only passengers holding a valid passport or visa as identification with images stored in the TVS photo gallery use the facial recognition system and all other identification credentials undergo a manual check by a direct foreign air carrier employee or authorized representative.
 3. Require all passengers using the TVS to undergo a biometric facial scan that will compare and match the facial scan of the passenger against the stored TVS database image of the passenger. The name of the passenger tendering the checked baggage to the direct employee or authorized representative must match the name appearing on the paper or mobile boarding pass and checked baggage destination tag(s) issued/printed in the Departure Control System.
 4. Prevent Inhibited Boarding Pass Printing Result (BPPR) passengers from using the TVS; and ensure they are referred to the foreign air carrier's direct employee or authorized representative for a manual passenger identification check as described in EA 1546-12-07 Series.
 5. Require all (b)(3):49 U.S.C. § 114(r)

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be released to persons without a "need to know" and is exempt from parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

3. The TVS matching thresholds meet or exceed the following:
 - a) True Match Rate of greater than or equal to 97 percent and;
 - b) False Match Rate/False Positive Identification Rate (FPIR) of less than or equal to 0.1 percent and;
 - c) False Non Match Rate (FNMR)/False Negative Identification Rate (FNIR) of less than or equal to 3 percent.
- B. The foreign air carrier's assigned International Industry Representative (IIR) and ATL's Federal Security Director (FSD) or designee must be immediately notified in the event of program information being misplaced or compromised during collection, storage, transmission, or disposal.
- C. Passenger Biometric Bag Drop
 1. The foreign air carrier must comply with the following procedures in lieu of those contained in EA 1546-12-07 Series, Section I.B.1.b., only when accepting checked baggage of passengers using valid government issued passports or visas verified by the TVS facial recognition system.
 2. Ensure that only passengers holding a valid passport or visa as identification with images stored in the TVS photo gallery use the facial recognition system and all other identification credentials undergo a manual check by a direct foreign air carrier employee or authorized representative.
 3. Require all passengers using the TVS to undergo a biometric facial scan that will compare and match the facial scan of the passenger against the stored TVS database image of the passenger. The name of the passenger tendering the checked baggage to the direct employee or authorized representative must match the name appearing on the paper or mobile boarding pass and checked baggage destination tag(s) issued/printed in the Departure Control System.
 4. Prevent Inhibited Boarding Pass Printing Result (BPPR) passengers from using the TVS; and ensure they are referred to the foreign air carrier's direct employee or authorized representative for a manual passenger identification check as described in EA 1546-12-07 Series.
 5. Require all (b)(3);49 U.S.C. § 114(r) (b)(3);49 U.S.C. § 114(r)
 6. Direct passengers who fail the biometric match at the TVS to a direct employee or authorized representative for manual passenger identification check and checked baggage acceptance as described in EA 1546-12-07 Series.

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be released to persons without a "need to know" as determined by 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unintentional release may result in civil penalty or other action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

3. The TVS matching thresholds meet or exceed the following:
 - a) True Match Rate of greater than or equal to 97 percent and;
 - b) False Match Rate/False Positive Identification Rate (FPIR) of less than or equal to 0.1 percent and;
 - c) False Non Match Rate (FNMR)/False Negative Identification Rate (FNIR) of less than or equal to 3 percent.
- B. The foreign air carrier's assigned International Industry Representative (IIR) and ATL's Federal Security Director (FSD) or designee must be immediately notified in the event of program information being misplaced or compromised during collection, storage, transmission, or disposal.
- C. Passenger Biometric Bag Drop
 1. The foreign air carrier must comply with the following procedures in lieu of those contained in EA 1546-12-07 Series, Section I.B.1.b., only when accepting checked baggage of passengers using valid government issued passports or visas verified by the TVS facial recognition system.
 2. Ensure that only passengers holding a valid passport or visa as identification with images stored in the TVS photo gallery use the facial recognition system and all other identification credentials undergo a manual check by a direct foreign air carrier employee or authorized representative.
 3. Require all passengers using the TVS to undergo a biometric facial scan that will compare and match the facial scan of the passenger against the stored TVS database image of the passenger. The name of the passenger tendering the checked baggage to the direct employee or authorized representative must match the name appearing on the paper or mobile boarding pass and checked baggage destination tag(s) issued/printed in the Departure Control System (DCS).
 4. Prevent Inhibited Boarding Pass Printing Result (BPPR) passengers from using the TVS; and ensure they are referred to the foreign air carrier's direct employee or authorized representative for a manual passenger identification check as described in EA 1546-12-07 Series.
 5. Require all (b)(3)-49 U.S.C. § 114(r) (b)(3)-49 U.S.C. § 114(r)
 6. Direct passengers who fail the biometric match at the TVS to a direct employee or authorized representative for manual passenger identification check and checked baggage acceptance as described in EA 1546-12-07 Series.

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be released to persons without a "need to know" as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

3. The TVS matching thresholds meet or exceed the following:
 - a) True Match Rate of greater than or equal to 97 percent and;
 - b) False Match Rate/False Positive Identification Rate (FPIR) of less than or equal to 0.1 percent and;
 - c) False Non Match Rate (FNMR)/False Negative Identification Rate (FNIR) of less than or equal to 3 percent.
- B. The foreign air carrier's assigned International Industry Representative (IIR) and ATL's Federal Security Director (FSD) or designee must be immediately notified in the event of program information being misplaced or compromised during collection, storage, transmission, or disposal.
- C. Passenger Biometric Bag Drop
 1. The foreign air carrier must comply with the following procedures in lieu of those contained in EA 1546-12-07 Series, Section I.B.1.b., only when accepting checked baggage of passengers using valid government issued passports or visas verified by the TVS facial recognition system.
 2. Ensure that only passengers holding a valid passport or visa as identification with images stored in the TVS photo gallery use the facial recognition system and all other identification credentials undergo a manual check by a direct foreign air carrier employee or authorized representative.
 3. Require all passengers using the TVS to undergo a biometric facial scan that will compare and match the facial scan of the passenger against the stored TVS database image of the passenger. The name of the passenger tendering the checked baggage to the direct employee or authorized representative must match the name appearing on the paper or mobile boarding pass and checked baggage destination tag(s) issued/printed in the Departure Control System.
 4. Prevent Inhibited Boarding Pass Printing Result (BPPR) passengers from using the TVS; and ensure they are referred to the foreign air carrier's direct employee or authorized representative for a manual passenger identification check as described in EA 1546-12-07 Series.
 5. Require all (b)(3):49 U.S.C. § 114(r) (b)(3):49 U.S.C. § 114(r)
 6. Direct passengers who fail the biometric match at the TVS to a direct employee or authorized representative for manual passenger identification check and checked baggage acceptance as described in EA 1546-12-07 Series.

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be released to persons without a "need to know" as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

3. The TVS matching thresholds meet or exceed the following:
 - a) True Match Rate of greater than or equal to 97 percent and;
 - b) False Match Rate/False Positive Identification Rate (FPIR) of less than or equal to 0.1 percent and;
 - c) False Non Match Rate (FNMR)/False Negative Identification Rate (FNIR) of less than or equal to 3 percent.
- B. The foreign air carrier's assigned International Industry Representative (IIR) and ATL's Federal Security Director (FSD) or designee must be immediately notified in the event of program information being misplaced or compromised during collection, storage, transmission, or disposal.
- C. Passenger Biometric Bag Drop
 1. The foreign air carrier must comply with the following procedures in lieu of those contained in EA 1546-12-07 Series, Section I.B.1.b., only when accepting checked baggage of passengers using valid government issued passports or visas verified by the TVS facial recognition system.
 2. Ensure that only passengers holding a valid passport or visa as identification with images stored in the TVS photo gallery use the facial recognition system and all other identification credentials undergo a manual check by a direct foreign air carrier employee or authorized representative.
 3. Require all passengers using the TVS to undergo a biometric facial scan that will compare and match the facial scan of the passenger against the stored TVS database image of the passenger. The name of the passenger tendering the checked baggage to the direct employee or authorized representative must match the name appearing on the paper or mobile boarding pass and checked baggage destination tag(s) issued/printed in the Departure Control System (DCS).
 4. Prevent Inhibited Boarding Pass Printing Result (BPPR) passengers from using the TVS; and ensure they are referred to the foreign air carrier's direct employee or authorized representative for a manual passenger identification check as described in EA 1546-12-07 Series.
 5. Require all (b)(3):49 U.S.C. § 114(r)
(b)(3):49 U.S.C. § 114(r)
 6. Direct passengers who fail the biometric match at the TVS to a direct employee or authorized representative for manual passenger identification check and checked baggage acceptance as described in EA 1546-12-07 Series.

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be released to persons without a "need to know" as defined by 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalties or other action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

5. Require all (b)(3):49 U.S.C. § 114(r)
(b)(3):49 U.S.C. § 114(r)
 6. Direct passengers who fail the biometric match at the TVS to a direct employee or authorized representative for manual passenger identification check and checked baggage acceptance as described in AOSSP Section 4.2.
 7. Prevent the use of TVS by any passenger under 14 years of age traveling alone or with other travelers under the age of 14.
- D. Verbally notify the PSI and the ATL FSD or his designee within 24 hours of all TVS system data breaches, data losses or data exposure of biometric information.
- E. 6 months after the effective date of this amendment, the aircraft operator must submit to the PSI a diagnostic report detailing performance levels (including the False Positive Identification Rate – FPIR) of the baggage drop and specifics on collection, storage and transmission rates.
- F. This amendment for ASOA will be terminated if the Delta Air Lines’ proof of concept amendment for use of the TVS is terminated for any reason.
- G. Should the aircraft operator seek to change its provider of biometric identification services to one other than TVS, this amendment will be cancelled.
- H. ASOA may use TVS as authorized by this amendment but the liability for compliance with all TSA requirements remains with ASOA at all times.

SECURITY DIRECTIVES

When TSA issues a Security Directive (SD) requiring additional security measures, the aircraft operator must comply with any procedures concerning passenger identification and checked baggage acceptance. The aircraft operator must also inform its assigned Principal Security Inspector (PSI) or International Industry Representative (IIR), as appropriate, how it will implement such SD requirements.

SCOPE AND DURATION OF APPROVAL

- A. In accordance with title 49 of the Code of Federal Regulations (CFR), section 1544.105(b), this document amends the TSA-approved security program adopted by the aircraft operator in accordance with the requirements of 49 CFR 1544.101(a). As this amendment is part of

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be released to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

~~SENSITIVE SECURITY INFORMATION~~

5. Require all (b)(3):49 U.S.C. § 114(r) [redacted]
(b)(3):49 U.S.C. § 114(r) [redacted]
 6. Direct passengers who fail the biometric match at the TVS to a direct employee or authorized representative for manual passenger identification check and checked baggage acceptance as described in AOSSP Section 4.2.
 7. Prevent the use of TVS by any passenger under 14 years of age traveling alone or with other travelers under the age of 14.
- D. Verbally notify the PSI and the ATL FSD or his designee within 24 hours of all TVS system data breaches, data losses or data exposure of biometric information.
- E. 6 months after the effective date of this amendment, the aircraft operator must submit to the PSI a diagnostic report detailing performance levels (including the False Positive Identification Rate – FPIR) of the baggage drop and specifics on collection, storage and transmission rates.
- F. This amendment for C77A will be terminated if the Delta Air Lines’ proof of concept amendment for use of the TVS is terminated for any reason.
- G. Should the aircraft operator seek to change its provider of biometric identification services to one other than TVS, this amendment will be cancelled.
- H. C7AA may use TVS as authorized by this amendment but the liability for compliance with all TSA requirements remains with C7AA at all times.

SECURITY DIRECTIVES

When TSA issues a Security Directive (SD) requiring additional security measures, the aircraft operator must comply with any procedures concerning passenger identification and checked baggage acceptance. The aircraft operator must also inform its assigned Principal Security Inspector (PSI) or International Industry Representative (IIR), as appropriate, how it will implement such SD requirements.

SCOPE AND DURATION OF APPROVAL

- A. In accordance with title 49 of the Code of Federal Regulations (CFR), section 1544.105(b), this document amends the TSA-approved security program adopted by the aircraft operator in accordance with the requirements of 49 CFR 1544.101(a). As this amendment is part of

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be released to persons without a "need to know" as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

~~SENSITIVE SECURITY INFORMATION~~

2. The use of the TVS system, for purposes of providing services to the aircraft operator in connection with this proof of concept, meets or exceeds the information security standards specified and approved by TSA.
 3. The TVS matching thresholds meet or exceed the following:
 - a) True Match Rate of greater than or equal to 97 percent and;
 - b) False Match Rate/False Positive Identification Rate (FPIR) of less than or equal to 0.1 percent and;
 - c) False Non Match Rate (FNMR)/False Negative Identification Rate (FNIR) of less than or equal to 3 percent.
- B. The aircraft operator's assigned Principal Security Inspector (PSI) and ATL's Federal Security Director (FSD) or designee must be immediately notified in the event of program information being misplaced or compromised during collection, storage, transmission, or disposal.
- C. Passenger Biometric Bag Drop
1. The aircraft operator must comply with the following procedures in lieu of those contained in AOSSP Sections 4.2., 6.3., 6.4., 6.6., 7.2., 7.7.2., and 7.7.3. only when accepting checked baggage of passengers using valid government issued passports or visas verified by the TVS facial recognition system.
 2. Ensure that only passengers holding a valid passport or visa as identification with images stored in the TVS photo gallery use the facial recognition system and all other identification credentials undergo a manual check by a direct aircraft operator employee or authorized representative.
 3. Require all passengers using the TVS to undergo a biometric facial scan that will compare and match the facial scan of the passenger against the stored TVS database image of the passenger. The name of the passenger tendering the checked baggage to the direct employee or authorized representative must match the name appearing on the paper or mobile boarding pass and checked baggage destination tag(s) issued/printed in the Departure Control System.
 4. Prevent Inhibited Boarding Pass Printing Result (BPPR) passengers from using the TVS; and ensure they are referred to the aircraft operator's direct employee or authorized representative for a manual passenger identification check as described in AOSSP Section 4.2.
 5. Require all (b)(3)-49 U.S.C. § 114(r)

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be released to persons without a "need to know" as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalties or other action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

~~SENSITIVE SECURITY INFORMATION~~

5. Require all (b)(3):49 U.S.C. § 114(r) [redacted]
(b)(3):49 U.S.C. § 114(r) [redacted]
 6. Direct passengers who fail the biometric match at the TVS to a direct employee or authorized representative for manual passenger identification check and checked baggage acceptance as described in AOSSP Section 4.2.
 7. Prevent the use of TVS by any passenger under 14 years of age traveling alone or with other travelers under the age of 14.
- D. Verbally notify the PSI and the ATL FSD or his designee within 24 hours of all TVS system data breaches, data losses or data exposure of biometric information.
- E. 6 months after the effective date of this amendment, the aircraft operator must submit to the PSI a diagnostic report detailing performance levels (including the False Positive Identification Rate – FPIR) of the baggage drop and specifics on collection, storage and transmission rates.
- F. This amendment for N6WA will be terminated if the Delta Air Lines' proof of concept amendment for use of the TVS is terminated for any reason.
- G. Should the aircraft operator seek to change its provider of biometric identification services to one other than TVS, this amendment will be cancelled.
- H. N6WA may use TVS as authorized by this amendment but the liability for compliance with all TSA requirements remains with N6WA at all times.

SECURITY DIRECTIVES

When TSA issues a Security Directive (SD) requiring additional security measures, the aircraft operator must comply with any procedures concerning passenger identification and checked baggage acceptance. The aircraft operator must also inform its assigned Principal Security Inspector (PSI) or International Industry Representative (IIR), as appropriate, how it will implement such SD requirements.

SCOPE AND DURATION OF APPROVAL

- A. In accordance with title 49 of the Code of Federal Regulations, section (CFR) 1544.105(b), this document amends the TSA-approved security program adopted by the aircraft operator in accordance with the requirements of 49 CFR 1544.101(a). As this amendment is part of

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be released to persons without a "need to know" as defined in 49 C.F.R. parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 and 1520.~~

~~SENSITIVE SECURITY INFORMATION~~

Section 4.2.

5. Require all (b)(3):49 U.S.C. § 114(r)
(b)(3):49 U.S.C. § 114(r)
 6. Direct passengers who fail the biometric match at the TVS to a direct employee or authorized representative for manual passenger identification check and checked baggage acceptance as described in AOSSP Section 4.2.
 7. Prevent the use of TVS by any passenger under 14 years of age traveling alone or with other travelers under the age of 14.
- D. Verbally notify the PSI and the ATL FSD or his designee within 24 hours of all TVS system data breaches, data losses or data exposure of biometric information.
- E. 6 months after the effective date of this amendment, the aircraft operator must submit to the PSI a diagnostic report detailing performance levels (including the False Positive Identification Rate – FPIR) of the baggage drop and specifics on collection, storage and transmission rates.
- F. This amendment for R61A will be terminated if the Delta Air Lines' proof of concept amendment for use of the TVS is terminated for any reason.
- G. Should the aircraft operator seek to change its provider of biometric identification services to one other than TVS, this amendment will be cancelled.
- H. R61A may use TVS as authorized by this amendment but the liability for compliance with all TSA requirements remains with R61A at all times.

SECURITY DIRECTIVES

When TSA issues a Security Directive (SD) requiring additional security measures, the aircraft operator must comply with any procedures concerning passenger identification and checked baggage acceptance. The aircraft operator must also inform its assigned Principal Security Inspector (PSI) or International Industry Representative (IIR), as appropriate, how it will implement such SD requirements.

SCOPE AND DURATION OF APPROVAL

- A. In accordance with title 49 of the Code of Federal Regulations (CFR), section 1544.105(b), this document amends the TSA-approved security program adopted by the aircraft operator in accordance with the requirements of 49 CFR 1544.101(a). As this amendment is part of

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be released to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

~~SENSITIVE SECURITY INFORMATION~~

5. Require all (b)(3):49 U.S.C. § 114(r)
(b)(3):49 U.S.C. § 114(r)
 6. Direct passengers who fail the biometric match at the TVS to a direct employee or authorized representative for manual passenger identification check and checked baggage acceptance as described in AOSSP Section 4.2.
 7. Prevent the use of TVS by any passenger under 14 years of age traveling alone or with other travelers under the age of 14.
- D. Verbally notify the PSI and the ATL FSD or his designee within 24 hours of all TVS system data breaches, data losses or data exposure of biometric information.
- E. Six months after the effective date of this amendment, the aircraft operator must submit to the PSI a diagnostic report detailing performance levels (including the False Positive Identification Rate – FPIR) of the baggage drop and specifics on collection, storage and transmission rates.
- F. This amendment for REXA will be terminated if the Delta Air Lines’ proof of concept amendment for the use of the TVS is terminated for any reason.
- G. Should the aircraft operator seek to change its provider of biometric identification services to one other than TVS, this amendment will be cancelled.
- H. REXA may use TVS as authorized by this amendment but the liability for compliance with all TSA requirements remains with REXA at all times.

SECURITY DIRECTIVES

When TSA issues a Security Directive (SD) requiring additional security measures, the aircraft operator must comply with any procedures concerning passenger identification and checked baggage acceptance. The aircraft operator must also inform its assigned Principal Security Inspector (PSI) or International Industry Representative (IIR), as appropriate, how it will implement such SD requirements.

SCOPE AND DURATION OF APPROVAL

- A. In accordance with title 49 of the Code of Federal Regulations (CFR), section 1544.105(b), this document amends the TSA-approved security program adopted by the aircraft operator in accordance with the requirements of 49 CFR 1544.101(a). As this amendment is part of

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be released to persons without a "need to know" as determined under parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. A prohibited release may result in civil penalties or other action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

SENSITIVE SECURITY INFORMATION

5. Require all (b)(3)-49 U.S.C. § 114(r)
(b)(3)-49 U.S.C. § 114(r)
 6. Direct passengers who fail the biometric match at the TVS to a direct employee or authorized representative for manual passenger identification check and checked baggage acceptance as described in AOSSP Section 4.2.
 7. Prevent the use of TVS by any passenger under 14 years of age traveling alone or with other travelers under the age of 14.
- D. Verbally notify the PSI and the ATL FSD or his designee within 24 hours of all TVS system data breaches, data losses or data exposure of biometric information.
- E. 6 months after the effective date of this amendment, the aircraft operator must submit to the PSI a diagnostic report detailing performance levels (including the False Positive Identification Rate – FPIR) of the baggage drop and specifics on collection, storage and transmission rates.
- F. This amendment for SWIA will be terminated if the Delta Air Lines' proof of concept amendment for use of the TVS is terminated for any reason.
- G. Should the aircraft operator seek to change its provider of biometric identification services to one other than TVS, this amendment will be cancelled.
- H. SWIA may use TVS as authorized by this amendment but the liability for compliance with all TSA requirements remains with SWIA at all times.

SECURITY DIRECTIVES

When TSA issues a Security Directive (SD) requiring additional security measures, the aircraft operator must comply with any procedures concerning passenger identification and checked baggage acceptance. The aircraft operator must also inform its assigned Principal Security Inspector (PSI) or International Industry Representative (IIR), as appropriate, how it will implement such SD requirements.

SCOPE AND DURATION OF APPROVAL

- A. In accordance with title 49 of the Code of Federal Regulations (CFR), section 1544.105(b), this document amends the TSA-approved security program adopted by the aircraft operator in accordance with the requirements of 49 CFR 1544.101(a). As this amendment is part of



Transportation Security Administration

U.S. Department of Homeland Security
Transportation Security Administration
601 South 12th Street
Arlington, VA 20598

EMERGENCY AMENDMENT ALTERNATIVE PROCEDURES

<u>FOREIGN AIR CARRIER</u>	Deutsche Lufthansa (DLAF)
<u>NUMBER</u>	AP-1546-12-01-DLAF-17-01A
<u>SUBJECT</u>	Self-Service Baggage Tagging (SSBT) Kiosks
<u>EMERGENCY AMENDMENT</u>	1546-12-01 series
<u>EFFECTIVE DATE</u>	March 31, 2018
<u>EXPIRATION DATE</u>	March 30, 2019
<u>SUPERSEDES</u>	AP-1546-12-01-DLAF-17-01
<u>LOCATIONS</u>	As Listed in Attachment 1

PURPOSE AND GENERAL INFORMATION

Subject to implementing the procedures outlined herein, the Transportation Security Administration (TSA) authorizes the foreign air carrier to conduct the Alternative Procedures (AP) contained in this document in lieu of the requirements contained in the Emergency Amendment (EA) 1546-12-01 series to: (1) compare a passenger's travel document with his/her valid passport or valid government-issued photo identification when tendering checked baggage, and (2) to ensure that checked baggage is only accepted by a direct air carrier employee or by an authorized representative. The foreign air carrier agrees to use the approved procedures below while it **continues to develop** a plan to explore the implementation of biometric technology to verify the identity of the passenger when tendering checked baggage using a self-service baggage tagging (SSBT) kiosk. This plan **has** a timeline for implementation, and the foreign air carrier **must submit quarterly reports to TSA as part of a request for a renewal of the AP.**

APPROVED PROCEDURES

The foreign air carrier must ensure that the following security measures are performed when permitting passengers to use an SSBT kiosk to print and apply checked baggage destination tags to their checked baggage, and introduce the checked baggage into the Hold Baggage Screening (HBS) system:

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be released to persons without a "need to know" as defined by 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

- A. **In lieu of the required baggage acceptance locations at ticket counters and boarding gates, in accordance with EA 1546-12-01 series, Section I.B.1., allow passengers with valid passports to check their baggage using the SSBT kiosks, as described in this AP.**
- B. **In lieu of the required passenger identification (ID) check performed by a foreign air carrier direct employee under EA 1546-12-01 series, Section I.B.1., require all passengers that use the SSBT kiosks to swipe a machine-readable passport at the self-service check-in kiosk to obtain their boarding pass. Passengers must swipe this boarding pass at the SSBT kiosk to obtain baggage destination tags. If the check-in kiosk is unable to read the passenger's passport, the passenger must not be permitted to use the SSBT kiosk.**
- C. **Prevent the use of the SSBT kiosks by any passenger under 18 years of age.**
- D. Prior to allowing passengers to use a SSBT kiosk to print and attach checked baggage destination tags, the foreign air carrier must notify passengers who wish to transport firearms in their checked baggage that they cannot use a SSBT kiosk and must tender their checked baggage at the foreign air carrier's airport check-in counter.
- E. **The passenger must be checked-in at the airport prior to using a SSBT kiosk. The barcode incorporated into the boarding pass must be used at the SSBT kiosk to generate the appropriate number of baggage tags.**
- F. The foreign air carrier must ensure that only checked baggage belonging to a passenger with a "cleared" or "selectee" Secure Flight Boarding Pass Print Result (BPPR) is accepted at a SSBT kiosk. Passengers with an "inhibited" or "error" BPPR must be prompted to see a direct air carrier employee or authorized representative at the foreign air carrier's airport check-in counter to tender checked baggage.
- G. The foreign air carrier must ensure that the SSBT kiosks prevent a passenger from checking-in more than the allowed number of checked baggage noted on the passenger's reservation, and prompt the passenger to see a direct air carrier employee or authorized representative at the foreign air carrier's airport check-in counter for acceptance of excess checked baggage. **Ensure that each individual inducts only his or her checked baggage and does not induct any other individual's baggage.**
- H. The foreign air carrier must prevent unauthorized access to the checked baggage after the passenger has loaded his/her checked baggage onto the baggage belt for transport and the checked baggage is accepted into the HBS.
- I. Ensure that direct employees or authorized representatives are in the immediate vicinity of the SSBT kiosks to monitor and ensure that all procedures in this AP are met.

- J. **No later than June 30th, 2018, and every ninety-days thereafter, the foreign air carrier must provide to its assigned International Industry Representative a quarterly check-in report, providing details of its evaluation of biometric technology and progress toward achieving an acceptable biometrics-based solution for identifying passengers checking baggage to verify the identity of passengers when tendering checked baggage using SSBT kiosks.**
- K. **The first report must include the following information:**
1. **An explanation of how travel documents, identity documents, and any government conducted background check information are linked and/or validated by the system and accomplished at the SSBT kiosk,**
 2. **An explanation of how the system guards against “Inhibited” or “Error” passengers receiving a baggage tag through the SSBT kiosk,**
 3. **A description of the procedures in place for the processing of passengers who fail the biometric match at the SSBT kiosk,**
 4. **The results of testing of the technology and system performance measures, to include the False Positive Rate,**
 5. **A description of all software used to process the passenger’s biographic and biometric information collected by the system. Provide data regarding the reliability and accuracy of the software, including conformance to industry standards and third party validation of the software,**
 6. **An explanation of enrollment into the DLAF biometric system including:**
 - a. **Whether all passengers must enroll in the system or enrollment into the system is limited (e.g., only Lufthansa frequent flyers can enroll)**
 - b. **What elements of biographic and biometric information is collected from the passenger,**
 - c. **Who performs the passenger enrollment (e.g., airline personnel, a third party contractor, or other) into the system,**
 - d. **What, if any, background checks are conducted on the passenger, and by whom (e.g., is it commercial or governmental),**

- e. **An explanation of the process employed by the foreign air carrier or its authorized representative to ensure that the individual who is enrolled is actually the individual who is represented to be.**

- 7. **A description of the security protocols in place to protect the system from cyber-attack and the evaluation of the reliability of the information technology systems used.**

- 8. **Identify who maintains/updates the passenger data,**

- 9. **What, if any, background checks are conducted on an individual who maintains/updates passenger data, and**

- 10. **Provide the expected date of system completion and the anticipated date of system implementation.**

- L. **The quarterly check-in reports must include:**
 - 1. **Updates to the information in K.1. thru 10. above,**

 - 2. **The results of any system testing conducted since the last submitted quarterly progress report, and**

 - 3. **The number of passengers that were processed through the SSBT kiosk.**

- M. **A renewal of this AP is contingent upon the foreign air carrier's implementation of a plan to incorporate biometric technology into its SSBT kiosk operations.**

DISSEMINATION REQUIRED

The foreign air carrier must immediately pass the information and measures set forth in this AP to all personnel necessary to implement and ensure compliance with this AP. The foreign air carrier must brief all individuals receiving Sensitive Security Information (SSI) on the restrictions governing dissemination. The TSA Administrator must approve any other dissemination. Title 49 of the Code of Federal Regulations (CFR), part 1520, prohibits unauthorized dissemination of this document or information contained herein.

DURATION OF APPROVAL

TSA may cancel this AP at any time. **TSA will cancel this AP if it concludes that the quarterly check-in reports required herein do not demonstrate adequate progress toward a biometrics-based solution for identifying passengers checking baggage that is acceptable,**

which determination is solely within TSA's discretion. This AP expires automatically at the end of the calendar day listed under "Expiration Date" above. The foreign air carrier must submit a written request for renewal to its assigned International Industry Representative a minimum of 45 calendar days prior to the expiration date.



Eddie D. Mayenschein
Assistant Administrator
Office of Security Policy and Industry Engagement

ATTACHMENT 1

1. Frankfurt Airport (FRA), Frankfurt am Main, Germany
2. Munich Airport (MUC), Munich, Germany



Transportation
Security
Administration

U.S. Department of Homeland Security
Transportation Security Administration
601 South 12th Street
Arlington, VA 20598

EMERGENCY AMENDMENT ALTERNATIVE PROCEDURES

FOREIGN AIR CARRIER Deutsche Lufthansa (DLAF)
NUMBER AP-1546-12-01-DLAF-17-01C
SUBJECT Self-Service Baggage Tagging (SSBT) Kiosks
EMERGENCY AMENDMENT EA 1546-12-01 series
EFFECTIVE DATE July 2, 2019
EXPIRATION DATE July 7, 2020
SUPERSEDES AP-1546-12-01-DLAF-17-01B
LOCATIONS As listed in Attachment 1

PURPOSE AND GENERAL INFORMATION

Subject to implementing the procedures outlined herein, the Transportation Security Administration (TSA) authorizes the foreign air carrier to conduct the Alternative Procedures (AP) contained in this document in lieu of the requirements contained in the Emergency Amendment (EA) 1546-12-01 series to: (1) compare a passenger's travel document with his/her valid passport or valid government-issued photo identification (ID) when tendering checked baggage, and (2) to ensure that checked baggage is only accepted by a direct air carrier employee or by an authorized representative. The foreign air carrier **must** use the approved procedures below, **including the established U.S. Customs and Border Protection (CBP) Traveler Verification System (TVS) performance requirements and passenger biometric bag drop procedures**, while it continues to **carry out the biometric technology pilot program** to verify the identity of the passenger when tendering checked baggage using a self-service baggage tagging (SSBT) kiosk. **The foreign air carrier may use the TVS biometric technology as authorized by this AP, but the liability for compliance with all TSA requirements remains with the foreign air carrier at all times. TSA's authorization is conditional upon the foreign air carrier's affirmative representation of certain security measures that are performed by the foreign air carrier in the terminal in which the SSBT operates. The foreign air carrier must deliver to TSA a technical description of these measures, as specified by its International Industry Representative (IIR) by July 22, 2019. If the foreign air carrier fails to do so, or if the measures described do not corroborate the foreign air carrier's representations, TSA may cancel this amendment in accordance with the Duration of Approval paragraph below.**

APPROVED PROCEDURES

The foreign air carrier must ensure that the following security measures are performed when permitting passengers to use **TVS and** a SSBT kiosk to print and apply checked baggage destination tags to their checked baggage and introduce the checked baggage into the Hold Baggage Screening (HBS) system:

A. Performance Requirements

The foreign air carrier must ensure:

- 1. Biographic and biometric data collected by the TVS from participating passengers is maintained, transmitted, and disposed of in a manner which prevents unauthorized access and/or release of information.**
- 2. A draft Test and Evaluation (T&E) plan is provided to its assigned International Industry Representative (IIR) within two months of the issuance of this AP. The T&E plan must be reviewed and approved by TSA and should clearly define:**
 - a. System components performing operations,**
 - b. Methodology to collect required data to demonstrate adherence to requirements,**
 - c. Reporting time table for initial evaluation results and periodic quality assessments,**
 - d. Configuration Management details on the configuration of the system under which the data were collected, including (but not necessarily limited to):**
 - 1) Software version numbers for TVS and for the software that it touches,**
 - 2) Face-matching algorithm version number (if it is separate from the rest of the software),**
 - 3) Camera make, model, and firmware,**
 - 4) Computers (make and model), operating systems (edition, version, OS Build), and hard drive images, and**
 - 5) Network server information.**
- 3. The foreign carrier must provide performance data collected from the activities described in paragraph 2. above to the IIR on a monthly basis.**

4. **The foreign air carrier baggage handling system must not impact or diminish TSA performance requirements:**
 - a. **True Match Rate of greater than or equal to 97 percent, and**
 - b. **False Match Rate/False Positive (FPIR) of less than or equal to 0.1 percent.**

B. Passenger Biometric Bag Drop/SSBT Procedures

1. In lieu of the required baggage acceptance locations at ticket counters and boarding gates, in accordance with EA 1546-12-01 series, Section I.B.1., **the foreign air carrier may** allow passengers with valid passports to check their baggage using TVS and the SSBT kiosks, as described in this AP.
2. In lieu of the required passenger ID check performed by a foreign air carrier direct employee under EA 1546-12-01 series, Section I.B.1., **the foreign carrier must:**
 - a. **Ensure passengers who use the TVS facial recognition system and who do not receive a match undergo a manual ID check and tender their checked baggage at the foreign air carrier’s airport check-in counter.**
 - b. **Require all passengers who use TVS and the SSBT kiosks to have a photograph taken that the TVS system will compare and match to reference the photos of the passenger stored in the TVS database. The name of the passenger tendering the baggage must match the name appearing on the boarding pass and checked baggage destination tag(s) issued/printed in the Departure Control System,**
3. **The foreign air carrier must** prevent the use of **TVS and** the SSBT kiosks by any passenger under 18 years of age.
4. Prior to allowing passengers to use **TVS and** a SSBT kiosk to print and attach checked baggage destination tags, the foreign air carrier must notify passengers who wish to transport firearms in their checked baggage that they cannot use a SSBT kiosk and must tender their checked baggage at the foreign air carrier’s airport check-in counter.
5. **The foreign air carrier must ensure the passenger is** checked-in prior to using **TVS and** a SSBT kiosk. The barcode incorporated into the boarding pass must be used at the SSBT kiosk to generate the appropriate number of baggage tags.
6. The foreign air carrier must ensure that only checked baggage belonging to a passenger with a “cleared” or “selectee” Secure Flight Boarding Pass Print Result (BPPR) is accepted at a SSBT kiosk. Passengers with an “inhibited” or “error” BPPR

must be prompted to see a direct air carrier employee or authorized representative at the foreign air carrier's airport check-in counter to tender checked baggage **and undergo a manual ID check as described in EA 1546-12-01 series.**

7. **The foreign air carrier must ensure that:**
 - a. **The SSBT kiosks prevent a passenger from checking-in more than the allowed number of checked baggage noted on the passenger's reservation, and prompt the passenger to see a direct air carrier employee or authorized representative at the foreign air carrier's airport check-in counter for acceptance of excess checked baggage, and**
 - b. **Each individual inducts only his or her checked baggage and does not induct any other individual's baggage.**
8. The foreign air carrier must prevent unauthorized access to the checked baggage after the passenger has loaded his/her checked baggage onto the baggage belt for transport and the checked baggage is accepted into the HBS.
9. **The foreign air carrier must** ensure that direct employees or authorized representatives are in the immediate vicinity of the SSBT kiosks to monitor and ensure that all procedures in this AP are met.

C. Monthly Reporting Requirements

1. **The foreign air carrier must continue to provide to its assigned IIR a monthly check-in report, providing details of its evaluation of biometric technology and progress toward achieving an acceptable biometrics-based solution for identifying passengers checking baggage to verify the identity of passengers when tendering checked baggage using TVS and the SSBT kiosks.**
2. The reports must include the following information:
 - a. An explanation of how travel documents, identity documents, and any government conducted background check information is linked and/or validated by the system and accomplished at the SSBT kiosk,
 - b. An explanation of how the system guards against "Inhibited" or "Error" passengers receiving a baggage tag through the SSBT kiosk,
 - c. A description of the procedures in place for the processing of passengers who fail the biometric match at the SSBT kiosk,
 - d. **The diagnostic report detailing results of testing of the technology and system performance measures, to include FPIR, of the baggage drop and specifics on**

collection, storage, and transmission rates.

- e. **Regarding configuration management details and/or changes to the configuration of the system, an explanation of enrollment into the DLAF biometric system including:**
 - 1) **Whether all passengers must enroll in the system or enrollment into the system is limited (e.g., only Lufthansa frequent flyers can enroll),**
 - 2) **What elements of biographic and biometric information is collected from the passenger,**
 - 3) **Who performs the passenger enrollment (e.g., foreign air carrier personnel, a third party contractor, or other) into the system,**
 - 4) **What, if any, background checks are conducted on the passenger, and by whom (e.g., is it commercial or governmental),**
 - 5) **An explanation of the process employed by the foreign air carrier or its authorized representative to ensure that the individual who is enrolled is actually the individual who is represented to be.**
- f. A description of the security protocols in place to protect the system from cyber-attack and the evaluation of the reliability of the information technology systems used.
- g. The identity of the party or parties responsible for the maintenance of updates to the passenger data,
- h. A description of what, if any, background checks are conducted on an individual who maintains/updates passenger data, and
- i. The expected date of system completion and the anticipated date of **full** system implementation.

3. Each monthly report submitted must include:

- a. **Updates to the information in C.2.a. through i. above,**
- b. The results of any system testing conducted since the last submitted progress report, and
- c. The number of passengers that were processed through TVS and the SSBT kiosk.

4. The foreign air carrier must note any changes from the previous month's report.

- D. **Based on the security measures that are performed by the foreign air carrier and/or the host government in the terminal in which the SSBT operates, and the foreign air carrier's continued implementation of biometric solutions, passengers using the SSBT kiosks may continue to do so without undergoing a manual ID check.**

- E. **Renewal of this AP is contingent upon the foreign air carrier's implementation of a TSA-approved plan to incorporate TVS biometric technology into its SSBT kiosk operations. This plan must have a timeline for implementation, and the foreign air carrier must submit monthly reports to TSA.**

- F. **The foreign air carrier must notify its assigned IIR:**
 - 1. **Immediately in the event of program information being misplaced or compromised during collection, storage, transmission, or disposal,**

 - 2. **Verbally, within 24-hours, of all TVS system data breaches, data losses, or data exposure of biometric information.**

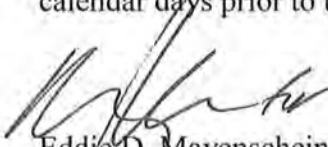
- G. **Change of Provider: should the foreign air carrier seek to change its provider of biometric identification services to one other than TVS, the foreign air carrier must notify its assigned IIR immediately.**

DISSEMINATION REQUIRED

The foreign air carrier must immediately pass the information and measures set forth in this Alternative Procedure (AP) to all personnel necessary to implement and ensure compliance with this AP. The foreign air carrier must brief all individuals receiving Sensitive Security Information (SSI) on the restrictions governing dissemination. The TSA Administrator must approve any other dissemination. Title 49 of the Code of Federal Regulations (CFR) part 1520 prohibits unauthorized dissemination of this document or information contained herein.

DURATION OF APPROVAL

TSA may cancel this AP at any time. This AP expires automatically at the end of the calendar day listed under expiration date above. The foreign air carrier must submit a written request for renewal to its assigned International Industry Representative a minimum of forty-five (45) calendar days prior to the expiration date.



Eddie D. Mayenschein
Assistant Administrator
Policy, Plans, and Engagement

ATTACHMENT 1

1. Frankfurt Airport (FRA), Frankfurt am Main, Germany
2. Munich Airport (MUC), Munich, Germany

~~SENSITIVE SECURITY INFORMATION~~



**Transportation
Security
Administration**

U.S. Department of Homeland Security
Transportation Security Administration
601 South 12th Street
Arlington, VA 20598

EMERGENCY AMENDMENT ALTERNATIVE PROCEDURES

FOREIGN AIR CARRIER AeroMexico (ASMF)
NUMBER AP-1546-12-07-ASMF-18-01
SUBJECT Biometric Identification Check- Checked Baggage Drop
EMERGENCY AMENDMENT EA 1546-12-07 Series, Sections I.B.1.b.
EFFECTIVE DATE December 1, 2018
EXPIRATION DATE November 30, 2019
SUPERSEDES Not Applicable
LOCATIONS Atlanta Hartsfield-Jackson International Airport (ATL)

PURPOSE AND GENERAL INFORMATION

This amendment allows the aircraft operator to use a bag drop system utilizing the Customs and Border Protection's (CBP) Traveler Verification Service (TVS) for passenger identification via facial recognition. The aircraft operator may accept and process checked baggage for flights departing from Atlanta Hartsfield-Jackson International Airport (ATL) without performing the passenger identification (ID) check and checked baggage acceptance measures as required in Sections 4.2., 6.3., 6.4., 6.6., 7.2., 7.7.2., and 7.7.3. of the Aircraft Operator Standard Security Program (AOSSP). This amendment is valid for one year while the Transportation Security Administration (TSA) evaluates the efficacy of these approved procedures under a proof of concept.

APPROVED PROCEDURES

A. TVS Performance Requirements

The foreign air carrier must ensure:

1. Biographic and biometric data collected by the TVS from participating passengers is maintained, transmitted, and disposed of in a manner which prevents unauthorized access and/or release of the information.

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be released to persons without a "need to know" as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalties or other action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

~~SENSITIVE SECURITY INFORMATION~~

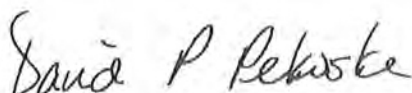
6. Direct passengers who fail the biometric match at the TVS to a direct employee or authorized representative for manual passenger identification check and checked baggage acceptance as described in EA 1546-12-07 Series.
 7. Prevent the use of TVS by any passenger under 14 years of age traveling alone or with other travelers under the age of 14.
- D. Verbally notify the IIR and the ATL FSD or his designee within 24 hours of all TVS system data breaches, data losses or data exposure of biometric information.
- E. 6 months after the effective date of this amendment, the foreign air carrier must submit to the IIR a diagnostic report detailing performance levels (including the False Positive Identification Rate – FPIR) of the baggage drop and specifics on collection, storage and transmission rates.
- F. This amendment for ASMF will be terminated if the Delta Air Lines' proof of concept amendment for use of the TVS is terminated for any reason.
- G. Should the foreign air carrier seek to change its provider of biometric identification services to one other than TVS, this amendment will be cancelled.
- H. ASMF may use TVS as authorized by this amendment but the liability for compliance with all TSA requirements remains with ASMF at all times.

DISSEMINATION REQUIRED

The foreign air carrier must immediately pass the information and measures set forth in this AP to all personnel necessary to implement and ensure compliance with this AP. The foreign air carrier must brief all individuals receiving Sensitive Security Information (SSI) on the restrictions governing dissemination. The TSA Administrator must approve any other dissemination. Title 49 of the Code of Federal Regulations (CFR), part 1520 prohibits unauthorized dissemination of this document or information contained herein.

DURATION OF APPROVAL

TSA may cancel this AP at any time. This AP expires automatically at the end of the calendar day listed under expiration date above. The foreign air carrier must submit a written request for renewal to its assigned IIR a minimum of forty-five (45) calendar days prior to the expiration date.



David P. Pecoske
Administrator

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be released to persons without a "need to know" authorization under 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalties or other action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~



**Transportation
Security
Administration**

U.S. Department of Homeland Security
Transportation Security Administration
601 South 12th Street
Arlington, VA 20598

EMERGENCY AMENDMENT ALTERNATIVE PROCEDURES

<u>FOREIGN AIR CARRIER</u>	Air France (CNFF)
<u>NUMBER</u>	AP-1546-12-07-CNFF-18-01
<u>SUBJECT</u>	Biometric Identification Check- Checked Baggage Drop
<u>EMERGENCY AMENDMENT</u>	EA 1546-12-07 Series, Sections I.B.1.b.
<u>EFFECTIVE DATE</u>	December 1, 2018
<u>EXPIRATION DATE</u>	November 30, 2019
<u>SUPERSEDES</u>	Not Applicable
<u>LOCATION</u>	Atlanta Hartsfield-Jackson International Airport (ATL)

PURPOSE AND GENERAL INFORMATION

This alternative procedure (AP) allows the foreign air carrier to use a bag drop system utilizing the Customs and Border Protection's (CBP) Traveler Verification Service (TVS) for passenger identification via facial recognition. The foreign air carrier may accept and process checked baggage for flights departing from Atlanta Hartsfield-Jackson International Airport (ATL) without performing the passenger identification (ID) check required by Emergency Amendment (EA) 1546-12-07 series. This alternative procedure is valid for one year while the Transportation Security Administration (TSA) evaluates the efficacy of these approved procedures under a proof of concept.

APPROVED PROCEDURES

A. TVS Performance Requirements

The foreign air carrier must ensure:

1. Biographic and biometric data collected by the TVS from participating passengers is maintained, transmitted, and disposed of in a manner which prevents unauthorized access and/or release of the information.
2. The use of the TVS system, for purposes of providing services to the foreign air carrier in connection with this proof of concept, meets or exceeds the information security standards specified and approved by TSA.

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be released to persons without a "need to know" as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

~~SENSITIVE SECURITY INFORMATION~~

7. Prevent the use of TVS by any passenger under 14 years of age traveling alone or with other travelers under the age of 14.
- D. Verbally notify the IIR and the ATL FSD or his designee within 24 hours of all TVS system data breaches, data losses or data exposure of biometric information.
- E. 6 months after the effective date of this amendment, the foreign air carrier must submit to the IIR a diagnostic report detailing performance levels (including the False Positive Identification Rate – FPIR) of the baggage drop and specifics on collection, storage and transmission rates.
- F. This amendment for CNFF will be terminated if the Delta Air Lines' proof of concept amendment for use of the TVS is terminated for any reason.
- G. Should the foreign air carrier seek to change its provider of biometric identification services to one other than TVS, this amendment will be cancelled.
- H. CNFF may use TVS as authorized by this amendment but the liability for compliance with all TSA requirements remains with CNFF at all times.

DISSEMINATION REQUIRED

The foreign air carrier must immediately pass the information and measures set forth in this AP to all personnel necessary to implement and ensure compliance with this AP. The foreign air carrier must brief all individuals receiving Sensitive Security Information (SSI) on the restrictions governing dissemination. The TSA Administrator must approve any other dissemination. Title 49 of the Code of Federal Regulations (CFR), part 1520 prohibits unauthorized dissemination of this document or information contained herein.

DURATION OF APPROVAL

TSA may cancel this AP at any time. This AP expires automatically at the end of the calendar day listed under expiration date above. The foreign air carrier must submit a written request for renewal to its assigned IIR a minimum of forty-five (45) calendar days prior to the expiration date.



David P. Pekoske
Administrator



**Transportation
Security
Administration**

U.S. Department of Homeland Security
Transportation Security Administration
601 South 12th Street
Arlington, VA 20598

EMERGENCY AMENDMENT ALTERNATIVE PROCEDURES

FOREIGN AIR CARRIER KLM Royal Dutch Airlines (KRDF)

NUMBER AP-1546-12-07-KRDF-18-01

SUBJECT Biometric Identification Check- Checked Baggage Drop

EMERGENCY AMENDMENT EA 1546-12-07 Series, Sections I.B.I.b.

EFFECTIVE DATE December 1, 2018

EXPIRATION DATE November 30, 2019

SUPERSEDES Not Applicable

LOCATIONS Atlanta Hartsfield-Jackson International Airport (ATL)

PURPOSE AND GENERAL INFORMATION

This alternative procedure (AP) allows the foreign air carrier to use a bag drop system utilizing the Customs and Border Protection's (CBP) Traveler Verification Service (TVS) for passenger identification via facial recognition. The foreign air carrier may accept and process checked baggage for flights departing from Atlanta Hartsfield-Jackson International Airport (ATL) without performing the passenger identification (ID) check required by Emergency Amendment (EA) 1546-12-07 series. This alternative procedure is valid for one year while the Transportation Security Administration (TSA) evaluates the efficacy of these approved procedures under a proof of concept.

APPROVED PROCEDURES

A. TVS Performance Requirements

The foreign air carrier must ensure:

1. Biographic and biometric data collected by the TVS from participating passengers is maintained, transmitted, and disposed of in a manner which prevents unauthorized access and/or release of the information.
2. The use of the TVS system, for purposes of providing services to the foreign air carrier in connection with this proof of concept, meets or exceeds the information security standards specified and approved by TSA.

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be released to persons without a "need to know" under 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

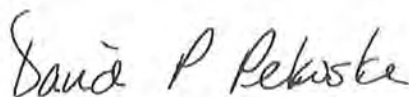
- 7. Prevent the use of TVS by any passenger under 14 years of age traveling alone or with other travelers under the age of 14.
- D. Verbally notify the IIR and the ATL FSD or his designee within 24 hours of all TVS system data breaches, data losses or data exposure of biometric information.
- E. 6 months after the effective date of this amendment, the foreign air carrier must submit to the IIR a diagnostic report detailing performance levels (including the False Positive Identification Rate – FPIR) of the baggage drop and specifics on collection, storage and transmission rates.
- F. This amendment for KRDF will be terminated if the Delta Air Lines' proof of concept amendment for use of the TVS is terminated for any reason.
- G. Should the foreign air carrier seek to change its provider of biometric identification services to one other than TVS, this amendment will be cancelled.
- H. KRDF may use TVS as authorized by this amendment but the liability for compliance with all TSA requirements remains with KRDF at all times.

DISSEMINATION REQUIRED

The foreign air carrier must immediately pass the information and measures set forth in this AP to all personnel necessary to implement and ensure compliance with this AP. The foreign air carrier must brief all individuals receiving Sensitive Security Information (SSI) on the restrictions governing dissemination. The TSA Administrator must approve any other dissemination. Title 49 of the Code of Federal Regulations (CFR), part 1520 prohibits unauthorized dissemination of this document or information contained herein.

DURATION OF APPROVAL

TSA may cancel this AP at any time. This AP expires automatically at the end of the calendar day listed under expiration date above. The foreign air carrier must submit a written request for renewal to its assigned IIR a minimum of forty-five (45) calendar days prior to the expiration date.



David P. Pekoske
Administrator



Transportation
Security
Administration

U.S. Department of Homeland Security
Transportation Security Administration
601 South 12th Street
Arlington, VA 20598

EMERGENCY AMENDMENT ALTERNATIVE PROCEDURES

FOREIGN AIR CARRIER Aerolitoral dba AeroMexico Connect (LVQF)

NUMBER AP-1546-12-07-LVQF-18-01

SUBJECT Biometric Identification Check- Checked Baggage Drop

EMERGENCY AMENDMENT EA 1546-12-07 Series, Sections I.B.1.b.

EFFECTIVE DATE December 1, 2018

EXPIRATION DATE November 30, 2019

SUPERSEDES Not Applicable

LOCATIONS Atlanta Hartsfield-Jackson International Airport (ATL)

PURPOSE AND GENERAL INFORMATION

This alternative procedure (AP) allows the foreign air carrier to use a bag drop system utilizing the Customs and Border Protection's (CBP) Traveler Verification Service (TVS) for passenger identification via facial recognition. The foreign air carrier may accept and process checked baggage for flights departing from Atlanta Hartsfield-Jackson International Airport (ATL) without performing the passenger identification (ID) check required by Emergency Amendment (EA) 1546-12-07 series. This alternative procedure is valid for one year while the Transportation Security Administration (TSA) evaluates the efficacy of these approved procedures under a proof of concept.

APPROVED PROCEDURES

A. TVS Performance Requirements

The foreign air carrier must ensure:

1. Biographic and biometric data collected by the TVS from participating passengers is maintained, transmitted, and disposed of in a manner which prevents unauthorized access and/or release of the information.
2. The use of the TVS system, for purposes of providing services to the foreign air carrier in connection with this proof of concept, meets or exceeds the information security standards specified and approved by TSA.

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be released to persons without a "need to know" as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalties and criminal action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

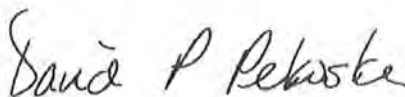
- 7. Prevent the use of TVS by any passenger under 14 years of age traveling alone or with other travelers under the age of 14.
- D. Verbally notify the IIR and the ATL FSD or his designee within 24 hours of all TVS system data breaches, data losses or data exposure of biometric information.
- E. 6 months after the effective date of this amendment, the foreign air carrier must submit to the IIR a diagnostic report detailing performance levels (including the False Positive Identification Rate – FPIR) of the baggage drop and specifics on collection, storage and transmission rates.
- F. This amendment for LVQF will be terminated if the Delta Air Lines' proof of concept amendment for use of the TVS is terminated for any reason.
- G. Should the foreign air carrier seek to change its provider of biometric identification services to one other than TVS, this amendment will be cancelled.
- H. LVQF may use TVS as authorized by this amendment but the liability for compliance with all TSA requirements remains with LVQF at all times.

DISSEMINATION REQUIRED

The foreign air carrier must immediately pass the information and measures set forth in this AP to all personnel necessary to implement and ensure compliance with this AP. The foreign air carrier must brief all individuals receiving Sensitive Security Information (SSI) on the restrictions governing dissemination. The TSA Administrator must approve any other dissemination. Title 49 of the Code of Federal Regulations (CFR), part 1520 prohibits unauthorized dissemination of this document or information contained herein.

DURATION OF APPROVAL

TSA may cancel this AP at any time. This AP expires automatically at the end of the calendar day listed under expiration date above. The foreign air carrier must submit a written request for renewal to its assigned IIR a minimum of forty-five (45) calendar days prior to the expiration date.



David P. Pecoske
Administrator



**Transportation
Security
Administration**

U.S. Department of Homeland Security
Transportation Security Administration
601 South 12th Street
Arlington, VA 20598

EMERGENCY AMENDMENT ALTERNATIVE PROCEDURES

FOREIGN AIR CARRIER Virgin Atlantic Ltd. (VAWF)

NUMBER AP-1546-12-07-VAWF-18-01

SUBJECT Biometric Identification Check- Checked Baggage Drop

EMERGENCY AMENDMENT EA 1546-12-07 Series, Sections I.B.1.b.

EFFECTIVE DATE December 1, 2018

EXPIRATION DATE November 30, 2019

SUPERSEDES Not Applicable

LOCATIONS Atlanta Hartsfield-Jackson International Airport (ATL)

PURPOSE AND GENERAL INFORMATION

This alternative procedure (AP) allows the foreign air carrier to use a bag drop system utilizing the Customs and Border Protection's (CBP) Traveler Verification Service (TVS) for passenger identification via facial recognition. The foreign air carrier may accept and process checked baggage for flights departing from Atlanta Hartsfield-Jackson International Airport (ATL) without performing the passenger identification (ID) check required by Emergency Amendment (EA) 1546-12-07 series. This alternative procedure is valid for one year while the Transportation Security Administration (TSA) evaluates the efficacy of these approved procedures under a proof of concept.

APPROVED PROCEDURES

A. TVS Performance Requirements

The foreign air carrier must ensure:

1. Biographic and biometric data collected by the TVS from participating passengers is maintained, transmitted, and disposed of in a manner which prevents unauthorized access and/or release of the information.
2. The use of the TVS system, for purposes of providing services to the foreign air carrier in connection with this proof of concept, meets or exceeds the information security standards specified and approved by TSA.

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be released to persons without a "need to know" as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil or criminal penalties or other action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

~~SENSITIVE SECURITY INFORMATION~~

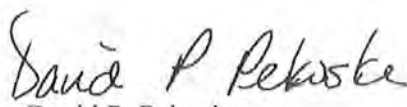
7. Prevent the use of TVS by any passenger under 14 years of age traveling alone or with other travelers under the age of 14.
- D. Verbally notify the IIR and the ATL FSD or his designee within 24 hours of all TVS system data breaches, data losses or data exposure of biometric information.
- E. 6 months after the effective date of this amendment, the foreign air carrier must submit to the IIR a diagnostic report detailing performance levels (including the False Positive Identification Rate – FPIR) of the baggage drop and specifics on collection, storage and transmission rates.
- F. This amendment for VAWF will be terminated if the Delta Air Lines' proof of concept amendment for use of the TVS is terminated for any reason.
- G. Should the foreign air carrier seek to change its provider of biometric identification services to one other than TVS, this amendment will be cancelled.
- H. VAWF may use TVS as authorized by this amendment but the liability for compliance with all TSA requirements remains with VAWF at all times.

DISSEMINATION REQUIRED

The foreign air carrier must immediately pass the information and measures set forth in this AP to all personnel necessary to implement and ensure compliance with this AP. The foreign air carrier must brief all individuals receiving Sensitive Security Information (SSI) on the restrictions governing dissemination. The TSA Administrator must approve any other dissemination. Title 49 of the Code of Federal Regulations (CFR), part 1520 prohibits unauthorized dissemination of this document or information contained herein.

DURATION OF APPROVAL

TSA may cancel this AP at any time. This AP expires automatically at the end of the calendar day listed under expiration date above. The foreign air carrier must submit a written request for renewal to its assigned IIR a minimum of forty-five (45) calendar days prior to the expiration date.


David P. Pekoske
Administrator

~~SENSITIVE SECURITY INFORMATION~~



Transportation
Security
Administration

U.S. Department of Homeland Security
Transportation Security Administration
601 South 12th Street
Arlington, VA 20598

TSA-APPROVED SECURITY PROGRAM AMENDMENT

AIRCRAFT OPERATOR ExpressJet Airlines (ASOA)
NUMBER ASOA-18-02
SUBJECT Biometric Identification Check – Checked Baggage Drop
PROGRAM 49 CFR 1544.101(a)
REFERENCE AOSSP Sections 4.2., 6.3., 6.4., 6.6., 7.2., 7.7.2., and 7.7.3.
LOCATION Atlanta Hartsfield-Jackson International Airport (ATL)
EFFECTIVE December 1, 2018
EXPIRES November 30, 2019
SUPERSEDES Not Applicable

PURPOSE AND GENERAL INFORMATION

This amendment allows the aircraft operator to use a bag drop system utilizing the Customs and Border Protection's (CBP) Traveler Verification Service (TVS) for passenger identification via facial recognition. The aircraft operator may accept and process checked baggage for flights departing from Atlanta Hartsfield-Jackson International Airport (ATL) without performing the passenger identification (ID) check and checked baggage acceptance measures as required in Sections 4.2., 6.3., 6.4., 6.6., 7.2., 7.7.2., and 7.7.3. of the Aircraft Operator Standard Security Program (AOSSP). This amendment is valid for one year while the Transportation Security Administration (TSA) evaluates the efficacy of these approved procedures under a proof of concept.

APPROVED PROCEDURES

A. TVS Performance Requirements

The aircraft operator must ensure:

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be released to persons without a "need to know" as determined by 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unlawful release may result in civil penalties or other action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

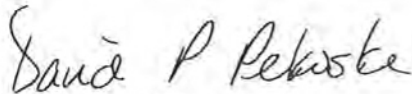
1. Biographic and biometric data collected by the TVS from participating passengers is maintained, transmitted, and disposed of in a manner which prevents unauthorized access and/or release of the information.
 2. The use of the TVS system, for purposes of providing services to the aircraft operator in connection with this proof of concept, meets or exceeds the information security standards specified and approved by TSA.
 3. The TVS matching thresholds meet or exceed the following:
 - a) True Match Rate of greater than or equal to 97 percent and;
 - b) False Match Rate/False Positive Identification Rate (FPIR) of less than or equal to 0.1 percent and;
 - c) False Non Match Rate (FNMR)/False Negative Identification Rate (FNIR) of less than or equal to 3 percent.
- B. The aircraft operator's assigned Principal Security Inspector (PSI) and ATL's Federal Security Director (FSD) or designee must be immediately notified in the event of program information being misplaced or compromised during collection, storage, transmission, or disposal.
- C. Passenger Biometric Bag Drop
1. The aircraft operator must comply with the following procedures in lieu of those contained in AOSSP Sections 4.2., 6.3., 6.4., 6.6., 7.2., 7.7.2., and 7.7.3, only when accepting checked baggage of passengers using valid government issued passports or visas verified by the TVS facial recognition system.
 2. Ensure that only passengers holding a valid passport or visa as identification with images stored in the TVS photo gallery use the facial recognition system and all other identification credentials undergo a manual check by a direct aircraft operator employee or authorized representative.
 3. Require all passengers using the TVS to undergo a biometric facial scan that will compare and match the facial scan of the passenger against the stored TVS database image of the passenger. The name of the passenger tendering the checked baggage to the direct employee or authorized representative must match the name appearing on the paper or mobile boarding pass and checked baggage destination tag(s) issued/printed in the Departure Control System.
 4. Prevent Inhibited Boarding Pass Printing Result (BPPR) passengers from using the TVS; and ensure they are referred to the aircraft operator's direct employee or authorized representative for a manual passenger identification check as described in AOSSP Section 4.2.

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be released to persons without a "need to know" as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

SENSITIVE SECURITY INFORMATION

the aircraft operator's TSA-approved security program, the aircraft operator must control accessibility and dissemination of this document in accordance with 49 CFR 1544.103(b).

- B. Changes to the AOSSP may require a corresponding revision of this amendment. It is the responsibility of the aircraft operator to review this amendment when a change to the AOSSP revises relevant requirements. Consult the assigned PSI or IIR, as appropriate, to determine if revision of this amendment is required.
- C. TSA may withdraw approval for use of this amendment without notice. Approval for use of this amendment expires at the end of the calendar day listed in the expiration date section above. The aircraft operator must submit a written request for renewal to the assigned PSI or IIR at least 45 calendar days prior to expiration.



David P. Pecoske
Administrator

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be released to persons without a "need to know" as defined by 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~



Transportation
Security
Administration

U.S. Department of Homeland Security
Transportation Security Administration
601 South 12th Street
Arlington, VA 20598

TSA-APPROVED SECURITY PROGRAM AMENDMENT

AIRCRAFT OPERATOR Compass Airlines (C77A)

NUMBER C77A-18-04

SUBJECT Biometric Identification Check – Checked Baggage Drop

PROGRAM 49 CFR 1544.101(a)

REFERENCE AOSSP Sections 4.2., 6.3., 6.4., 6.6., 7.2., 7.7.2., and 7.7.3.

LOCATION Atlanta Hartsfield-Jackson International Airport (ATL)

EFFECTIVE December 1, 2018

EXPIRES November 30, 2019

SUPERSEDES Not Applicable

PURPOSE AND GENERAL INFORMATION

This amendment allows the aircraft operator to use a bag drop system utilizing the Customs and Border Protection's (CBP) Traveler Verification Service (TVS) for passenger identification via facial recognition. The aircraft operator may accept and process checked baggage for flights departing from Atlanta Hartsfield-Jackson International Airport (ATL) without performing the passenger identification (ID) check and checked baggage acceptance measures as required in Sections 4.2., 6.3., 6.4., 6.6., 7.2., 7.7.2., and 7.7.3. of the Aircraft Operator Standard Security Program (AOSSP). This amendment is valid for one year while the Transportation Security Administration (TSA) evaluates the efficacy of these approved procedures under a proof of concept.

APPROVED PROCEDURES

A. TVS Performance Requirements

The aircraft operator must ensure:

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be released to persons without a "need to know" as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

1. Biographic and biometric data collected by the TVS from participating passengers is maintained, transmitted, and disposed of in a manner which prevents unauthorized access and/or release of the information.
 2. The use of the TVS system, for purposes of providing services to the aircraft operator in connection with this proof of concept, meets or exceeds the information security standards specified and approved by TSA.
 3. The TVS matching thresholds meet or exceed the following:
 - a) True Match Rate of greater than or equal to 97 percent and;
 - b) False Match Rate/False Positive Identification Rate (FPIR) of less than or equal to 0.1 percent and;
 - c) False Non Match Rate (FNMR)/False Negative Identification Rate (FNIR) of less than or equal to 3 percent.
- B. The aircraft operator's assigned Principal Security Inspector (PSI) and ATL's Federal Security Director (FSD) or designee must be immediately notified in the event of program information being misplaced or compromised during collection, storage, transmission, or disposal.
- C. Passenger Biometric Bag Drop
1. The aircraft operator must comply with the following procedures in lieu of those contained in AOSSP Sections 4.2., 6.3., 6.4., 6.6., 7.2., 7.7.2., and 7.7.3. only when accepting checked baggage of passengers using valid government issued passports or visas verified by the TVS facial recognition system.
 2. Ensure that only passengers holding a valid passport or visa as identification with images stored in the TVS photo gallery use the facial recognition system and all other identification credentials undergo a manual check by a direct aircraft operator employee or authorized representative.
 3. Require all passengers using the TVS to undergo a biometric facial scan that will compare and match the facial scan of the passenger against the stored TVS database image of the passenger. The name of the passenger tendering the checked baggage to the direct employee or authorized representative must match the name appearing on the paper or mobile boarding pass and checked baggage destination tag(s) issued/printed in the Departure Control System.
 4. Prevent Inhibited Boarding Pass Printing Result (BPPR) passengers from using the TVS; and ensure they are referred to the aircraft operator's direct employee or authorized representative for a manual passenger identification check as described in AOSSP Section 4.2.

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be released to persons without a "need to know" as defined in 49 C.F.R. parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 and 1520.~~

~~SENSITIVE SECURITY INFORMATION~~

the aircraft operator's TSA-approved security program, the aircraft operator must control accessibility and dissemination of this document in accordance with 49 CFR 1544.103(b),

- B. Changes to the AOSSP may require a corresponding revision of this amendment. It is the responsibility of the aircraft operator to review this amendment when a change to the AOSSP revises relevant requirements. Consult the assigned PSI or IIR, as appropriate, to determine if revision of this amendment is required.
- C. TSA may withdraw approval for use of this amendment without notice. Approval for use of this amendment expires at the end of the calendar day listed in the expiration date section above. The aircraft operator must submit a written request for renewal to the assigned PSI or IIR at least 45 calendar days prior to expiration.



David P. Pecoske
Administrator



Transportation
Security
Administration

U.S. Department of Homeland Security
Transportation Security Administration
601 South 12th Street
Arlington, VA 20598

TSA-APPROVED SECURITY PROGRAM AMENDMENT

AIRCRAFT OPERATOR Delta Air Lines (DALA)
NUMBER DALA-18-04
SUBJECT Biometric Identification Check – Checked Baggage Drop
PROGRAM 49 CFR 1544.101(a)
REFERENCE AOSSP Sections 4.2., 6.3., 6.4., 6.6., 7.2., 7.7.2., and 7.7.3.
LOCATION Atlanta Hartsfield-Jackson International Airport (ATL)
EFFECTIVE December 1, 2018
EXPIRES November 30, 2019
SUPERSEDES Not Applicable

PURPOSE AND GENERAL INFORMATION

This amendment allows the aircraft operator to use a bag drop system utilizing the Customs and Border Protection's (CBP) Traveler Verification Service (TVS) for passenger identification via facial recognition. The aircraft operator may accept and process checked baggage for flights departing from Atlanta Hartsfield-Jackson International Airport (ATL) without performing the passenger identification (ID) check and checked baggage acceptance measures as required in Sections 4.2., 6.3., 6.4., 6.6., 7.2., 7.7.2., and 7.7.3. of the Aircraft Operator Standard Security Program (AOSSP). This amendment is valid for one year while the Transportation Security Administration (TSA) evaluates the efficacy of these approved procedures under a proof of concept.

APPROVED PROCEDURES

A. TVS Performance Requirements

The aircraft operator must ensure:

1. Biographic and biometric data collected by the TVS from participating passengers is maintained, transmitted, and disposed of in a manner which prevents unauthorized access and/or release of the information.

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be released to persons without a "need to know" as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalties or criminal action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

~~SENSITIVE SECURITY INFORMATION~~

6. Direct passengers who fail the biometric match at the TVS to a direct employee or authorized representative for manual passenger identification check and checked baggage acceptance as described in AOSSP Section 4.2.
 7. Prevent the use of TVS by any passenger under 14 years of age traveling alone or with other travelers under the age of 14.
- D. Verbally notify the PSI and the ATL FSD or his designee within 24 hours of all TVS system data breaches, data losses or data exposure of biometric information.
- E. 6 months after the effective date of this amendment, the aircraft operator must submit to the PSI a diagnostic report detailing performance levels (including the False Positive Identification Rate – FPIR) of the baggage drop and specifics on collection, storage and transmission rates.
- F. Should the aircraft operator seek to change its provider of biometric identification services to one other than TVS, this amendment will be cancelled.
- G. DALA may use TVS as authorized by this amendment but the liability for compliance with all TSA requirements remains with DALA at all times.

SECURITY DIRECTIVES

When TSA issues a Security Directive (SD) requiring additional security measures, the aircraft operator must comply with any procedures concerning passenger identification and checked baggage acceptance. The aircraft operator must also inform its assigned Principal Security Inspector (PSI) or International Industry Representative (IIR), as appropriate, how it will implement such SD requirements.

SCOPE AND DURATION OF APPROVAL

- A. In accordance with title 49 of the Code of Federal Regulations (CFR), section 1544.105(b), this document amends the TSA-approved security program adopted by the aircraft operator in accordance with the requirements of 49 CFR 1544.101(a). As this amendment is part of the aircraft operator's TSA-approved security program, the aircraft operator must control accessibility and dissemination of this document in accordance with 49 CFR 1544.103(b).
- B. Changes to the AOSSP may require a corresponding revision of this amendment. It is the responsibility of the aircraft operator to review this amendment when a change to the AOSSP revises relevant requirements. Consult the assigned PSI or IIR, as appropriate, to determine if revision of this amendment is required.

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be released to persons without a "need to know" as defined in 49 C.F.R. parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalties or other action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 and 1520.~~

~~SENSITIVE SECURITY INFORMATION~~

- C. TSA may withdraw approval for use of this amendment without notice. Approval for use of this amendment expires at the end of the calendar day listed in the expiration date section above. The aircraft operator must submit a written request for renewal to the assigned PSI or IIR at least 45 calendar days prior to expiration.



David P. Pecoske
Administrator

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be released to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in a civil or criminal penalty or other action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~



Transportation
Security
Administration

U.S. Department of Homeland Security
Transportation Security Administration
601 South 12th Street
Arlington, VA 20598

TSA-APPROVED SECURITY PROGRAM AMENDMENT

AIRCRAFT OPERATOR GoJet Airlines (N6WA)
NUMBER N6WA-18-03
SUBJECT Biometric Identification Check – Checked Baggage Drop
PROGRAM 49 CFR 1544.101(a)
REFERENCE AOSSP Sections 4.2., 6.3., 6.4., 6.6., 7.2., 7.7.2., and 7.7.3.
LOCATION Atlanta Hartsfield-Jackson International Airport (ATL)
EFFECTIVE December 1, 2018
EXPIRES November 30, 2019
SUPERSEDES Not Applicable

PURPOSE AND GENERAL INFORMATION

This amendment allows the aircraft operator to use a bag drop system utilizing the Customs and Border Protection's (CBP) Traveler Verification Service (TVS) for passenger identification via facial recognition. The aircraft operator may accept and process checked baggage for flights departing from Atlanta Hartsfield-Jackson International Airport (ATL) without performing the passenger identification (ID) check and checked baggage acceptance measures as required in Sections 4.2., 6.3., 6.4., 6.6., 7.2., 7.7.2., and 7.7.3. of the Aircraft Operator Standard Security Program (AOSSP). This amendment is valid for one year while the Transportation Security Administration (TSA) evaluates the efficacy of these approved procedures under a proof of concept.

APPROVED PROCEDURES

A. TVS Performance Requirements

The aircraft operator must ensure:

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be released to persons without a "need to know" as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalties or other action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

~~SENSITIVE SECURITY INFORMATION~~

1. Biographic and biometric data collected by the TVS from participating passengers is maintained, transmitted, and disposed of in a manner which prevents unauthorized access and/or release of the information.
 2. The use of the TVS system, for purposes of providing services to the aircraft operator in connection with this proof of concept, meets or exceeds the information security standards specified and approved by TSA.
 3. The TVS matching thresholds meet or exceed the following:
 - a) True Match Rate of greater than or equal to 97 percent and;
 - b) False Match Rate/False Positive Identification Rate (FPIR) of less than or equal to 0.1 percent and;
 - c) False Non Match Rate (FNMR)/False Negative Identification Rate (FNIR) of less than or equal to 3 percent.
- B. The aircraft operator's assigned Principal Security Inspector (PSI) and ATL's Federal Security Director (FSD) or designee must be immediately notified in the event of program information being misplaced or compromised during collection, storage, transmission, or disposal.
- C. Passenger Biometric Bag Drop
1. The aircraft operator must comply with the following procedures in lieu of those contained in AOSSP Sections 4.2., 6.3., 6.4., 6.6., 7.2., 7.7.2., and 7.7.3. only when accepting checked baggage of passengers using valid government issued passports or visas verified by the TVS facial recognition system.
 2. Ensure that only passengers holding a valid passport or visa as identification with images stored in the TVS photo gallery use the facial recognition system and all other identification credentials undergo a manual check by a direct aircraft operator employee or authorized representative.
 3. Require all passengers using the TVS to undergo a biometric facial scan that will compare and match the facial scan of the passenger against the stored TVS database image of the passenger. The name of the passenger tendering the checked baggage to the direct employee or authorized representative must match the name appearing on the paper or mobile boarding pass and checked baggage destination tag(s) issued/printed in the Departure Control System (DCS).
 4. Prevent Inhibited Boarding Pass Printing Result (BPPR) passengers from using the TVS; and ensure they are referred to the aircraft operator's direct employee or authorized representative for a manual passenger identification check as described in AOSSP Section 4.2.

WARNING: This record contains Sensitive Security Information, as defined under 49 CFR parts 15 and 1520. No part of this record may be released to anyone, other than a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

~~SENSITIVE SECURITY INFORMATION~~

the aircraft operator's TSA-approved security program, the aircraft operator must control accessibility and dissemination of this document in accordance with 49 CFR 1544.103(b).

- B. Changes to the AOSSP may require a corresponding revision of this amendment. It is the responsibility of the aircraft operator to review this amendment when a change to the AOSSP revises relevant requirements. Consult the assigned PSI or IIR, as appropriate, to determine if revision of this amendment is required.
- C. TSA may withdraw approval for use of this amendment without notice. Approval for use of this amendment expires at the end of the calendar day listed in the expiration date section above. The aircraft operator must submit a written request for renewal to the assigned PSI or IIR at least 45 calendar days prior to expiration.



David P. Pekoske
Administrator

~~SENSITIVE SECURITY INFORMATION~~



**Transportation
Security
Administration**

U.S. Department of Homeland Security
Transportation Security Administration
601 South 12th Street
Arlington, VA 20598

TSA-APPROVED SECURITY PROGRAM AMENDMENT

AIRCRAFT OPERATOR Republic Airline (R61A)
NUMBER R61A-18-05
SUBJECT Biometric Identification Check – Checked Baggage Drop
PROGRAM 49 CFR 1544.101(a)
REFERENCE AOSSP Sections 4.2., 6.3., 6.4., 6.6., 7.2., 7.7.2., and 7.7.3.
LOCATION Atlanta Hartsfield-Jackson International Airport (ATL)
EFFECTIVE December 1, 2018
EXPIRES November 30, 2019
SUPERSEDES Not Applicable

PURPOSE AND GENERAL INFORMATION

This amendment allows the aircraft operator to use a bag drop system utilizing the Customs and Border Protection's (CBP) Traveler Verification Service (TVS) for passenger identification via facial recognition. The aircraft operator may accept and process checked baggage for flights departing from Atlanta Hartsfield-Jackson International Airport (ATL) without performing the passenger identification (ID) check and checked baggage acceptance measures as required in Sections 4.2., 6.3., 6.4., 6.6., 7.2., 7.7.2., and 7.7.3. of the Aircraft Operator Standard Security Program (AOSSP). This amendment is valid for one year while the Transportation Security Administration (TSA) evaluates the efficacy of these approved procedures under a proof of concept.

APPROVED PROCEDURES

A. TVS Performance Requirements

The aircraft operator must ensure:

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be released to persons without a "need to know" as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

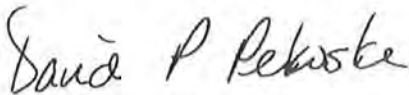
~~SENSITIVE SECURITY INFORMATION~~

1. Biographic and biometric data collected by the TVS from participating passengers is maintained, transmitted, and disposed of in a manner which prevents unauthorized access and/or release of the information.
 2. The use of the TVS system, for purposes of providing services to the aircraft operator in connection with this proof of concept, meets or exceeds the information security standards specified and approved by TSA.
 3. The TVS matching thresholds meet or exceed the following:
 - a) True Match Rate of greater than or equal to 97 percent and;
 - b) False Match Rate/False Positive Identification Rate (FPIR) of less than or equal to 0.1 percent and;
 - c) False Non Match Rate (FNMR)/False Negative Identification Rate (FNIR) of less than or equal to 3 percent.
- B. The aircraft operator's assigned Principal Security Inspector (PSI) and ATL's Federal Security Director (FSD) or designee must be immediately notified in the event of program information being misplaced or compromised during collection, storage, transmission, or disposal.
- C. Passenger Biometric Bag Drop
1. The aircraft operator must comply with the following procedures in lieu of those contained in AOSSP Sections 4.2., 6.3., 6.4., 6.6., 7.2., 7.7.2., and 7.7.3. only when accepting checked baggage of passengers using valid government issued passports or visas verified by the TVS facial recognition system.
 2. Ensure that only passengers holding a valid passport or visa as identification with images stored in the TVS photo gallery use the facial recognition system and all other identification credentials undergo a manual check by a direct aircraft operator employee or authorized representative.
 3. Require all passengers using the TVS to undergo a biometric facial scan that will compare and match the facial scan of the passenger against the stored TVS database image of the passenger. The name of the passenger tendering the checked baggage to the direct employee or authorized representative must match the name appearing on the paper or mobile boarding pass and checked baggage destination tag(s) issued/printed in the Departure Control System.
 4. Prevent Inhibited Boarding Pass Printing Result (BPPR) passengers from using the TVS; and ensure they are referred to the aircraft operator's direct employee or authorized representative for a manual passenger identification check as described in AOSSP

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be released to persons without a "need to know" as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of the Department. Unauthorized release may result in civil penalties or other actions. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

the aircraft operator's TSA-approved security program, the aircraft operator must control accessibility and dissemination of this document in accordance with 49 CFR 1544.103(b).

- B. Changes to the AOSSP may require a corresponding revision of this amendment. It is the responsibility of the aircraft operator to review this amendment when a change to the AOSSP revises relevant requirements. Consult the assigned PSI or IIR, as appropriate, to determine if revision of this amendment is required.
- C. TSA may withdraw approval for use of this amendment without notice. Approval for use of this amendment expires at the end of the calendar day listed in the expiration date section above. The aircraft operator must submit a written request for renewal to the assigned PSI or IIR at least 45 calendar days prior to expiration.



David P. Pekoske
Administrator

SENSITIVE SECURITY INFORMATION



Transportation
Security
Administration

U.S. Department of Homeland Security
Transportation Security Administration
601 South 12th Street
Arlington, VA 20598

TSA-APPROVED SECURITY PROGRAM AMENDMENT

AIRCRAFT OPERATOR Endeavor Air (REXA)

NUMBER REXA-18-03

SUBJECT Biometric Identification Check – Checked Baggage Drop

PROGRAM 49 CFR 1544.101(a)

REFERENCE AOSSP Sections 4.2., 6.3., 6.4., 6.6., 7.2., 7.7.2., and 7.7.3.

LOCATION Atlanta Hartsfield-Jackson International Airport (ATL)

EFFECTIVE December 1, 2018

EXPIRES November 30, 2019

SUPERSEDES Not Applicable

PURPOSE AND GENERAL INFORMATION

This amendment allows the aircraft operator to use a bag drop system utilizing the Customs and Border Protection's (CBP) Traveler Verification Service (TVS) for passenger identification via facial recognition. The aircraft operator may accept and process checked baggage for flights departing from Atlanta Hartsfield-Jackson International Airport (ATL) without performing the passenger identification (ID) check and checked baggage acceptance measures as required in Sections 4.2., 6.3., 6.4., 6.6., 7.2., 7.7.2., and 7.7.3. of the Aircraft Operator Standard Security Program (AOSSP). This amendment is valid for one year while the Transportation Security Administration (TSA) evaluates the efficacy of these approved procedures under a proof of concept.

APPROVED PROCEDURES

A. TVS Performance Requirements

The aircraft operator must ensure:

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be released to persons without a "need to know" as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

~~SENSITIVE SECURITY INFORMATION~~

1. Biographic and biometric data collected by the TVS from participating passengers is maintained, transmitted, and disposed of in a manner which prevents unauthorized access and/or release of the information.
 2. The use of the TVS system, for purposes of providing services to the aircraft operator in connection with this proof of concept, meets or exceeds the information security standards specified and approved by TSA.
 3. The TVS matching thresholds meet or exceed the following:
 - a) True Match Rate of greater than or equal to 97 percent and;
 - b) False Match Rate/False Positive Identification Rate (FPIR) of less than or equal to 0.1 percent and;
 - c) False Non Match Rate (FNMR)/False Negative Identification Rate (FNIR) of less than or equal to 3 percent.
- B. The aircraft operator's assigned Principal Security Inspector (PSI) and ATL's Federal Security Director (FSD) or designee must be immediately notified in the event of program information being misplaced or compromised during collection, storage, transmission, or disposal.
- C. Passenger Biometric Bag Drop
1. The aircraft operator must comply with the following procedures in lieu of those contained in AOSSP Sections 4.2., 6.3., 6.4., 6.6., 7.2., 7.7.2., and 7.7.3. only when accepting checked baggage of passengers using valid government issued passports or visas verified by the TVS facial recognition system.
 2. Ensure that only passengers holding a valid passport or visa as identification with images stored in the TVS photo gallery use the facial recognition system and all other identification credentials undergo a manual check by a direct aircraft operator employee or authorized representative.
 3. Require all passengers using the TVS to undergo a biometric facial scan that will compare and match the facial scan of the passenger against the stored TVS database image of the passenger. The name of the passenger tendering the checked baggage to the direct employee or authorized representative must match the name appearing on the paper or mobile boarding pass and checked baggage destination tag(s) issued/printed in the Departure Control System.
 4. Prevent Inhibited Boarding Pass Printing Result (BPPR) passengers from using the TVS; and ensure they are referred to the aircraft operator's direct employee or authorized representative for a manual passenger identification check as described in AOSSP Section 4.2.

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be released to persons without a "need to know" as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in a civil penalty or other action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

~~SENSITIVE SECURITY INFORMATION~~

the aircraft operator's TSA-approved security program, the aircraft operator must control accessibility and dissemination of this document in accordance with 49 CFR 1544.103(b).

- B. Changes to the AOSSP may require a corresponding revision of this amendment. It is the responsibility of the aircraft operator to review this amendment when a change to the AOSSP revises relevant requirements. Consult the assigned PSI or IIR, as appropriate, to determine if revision of this amendment is required.
- C. TSA may withdraw approval for use of this amendment without notice. Approval for use of this amendment expires at the end of the calendar day listed in the expiration date section above. The aircraft operator must submit a written request for renewal to the assigned PSI or IIR at least 45 calendar days prior to expiration.



David P. Pekoske
Administrator

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be released to persons without a "need to know" as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

U.S. Department of Homeland Security
601 South 12th Street
Arlington, VA 20598



Transportation
Security
Administration

AUG 22 2018

Jack Cohen
Manager of Security Compliance
JetBlue Airways
27-01 Queens Plaza North
Long Island City, NY 11101

Dear Mr. Cohen:

Thank you for the letter of April 30, 2018, on behalf of JetBlue Airways (JetBlue), requesting the Transportation Security Administration (TSA) consider an amendment of your Aircraft Operator Standard Security Program (AOSSP) allowing the use of a biometric facial recognition system to conduct identification (ID) verification. Specifically, your request is to utilize the Customs and Border Protection (CBP) Traveler Verification Service (TVS) at the self-service bag drop in John F. Kennedy Airport (JFK) in lieu of the required ID check of the passenger upon tendering checked baggage for transport as described in the AOSSP. It is TSA's role to consider whether JetBlue's proposed amendment to enhance the customer experience provides the same, or an improved, level of security commensurate to the passenger identification check required by the AOSSP. TSA has undertaken a review of your request and determined that the amendment decision is premature, and that some conditions must be met before approval.

In order to proceed on the path toward determining whether TSA will approve JetBlue's proposed amendment for a fully functional, self-service bag drop unit, JetBlue will need to demonstrate progress towards meeting TSA requirements, as discussed in the attached document. It is expected that JetBlue hire a trusted third party assessor, at its own expense and approved by TSA, to conduct a test in accordance with TSA requirements and provide a final report outlining the system's ability to meet TSA's requirements. Test data can be collected in an operational setting, absent a program amendment, provided the test system is operated in addition to JetBlue still performing the manual identification check of the passenger required in the AOSSP. Alternatively, JetBlue can build the test system in a controlled laboratory environment simulating live operations to collect the data – TSA will support either process. Additionally, TSA requests that JetBlue deliver a draft Quality Control Plan (QCP) defining the procedures and guidelines the aircraft operator will employ to monitor, measure, and report compliance with TSA requirements upon broader deployment of the system, including a process for managing and escalating non-compliance where needed.

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be released to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

2020-TSFO-00198_00704

To remain flexible and adaptable to new biometric technologies and threats, TSA also requests that JetBlue provide a report on live demonstration to their assigned Principal Security Inspector or International Industry Representative and relevant TSA technical experts at least once every 90 calendar days. As part of this process, JetBlue must demonstrate the security effectiveness and usability of the system under development (or test) to-date. This iterative process will enable TSA to proactively examine the system for technical, legal, and regulatory issues and provide JetBlue the timely feedback it needs to proceed with its amendment request. As JetBlue provides additional requested information, TSA will evaluate whether it is necessary to impose additional mitigation strategies or modify the existing policies, technology standards, and requirements. To avoid delays in consideration of your amendment, please provide the requested information as soon as practicable.

TSA looks forward to partnering with JetBlue to strengthen aviation security using new and increasingly more sophisticated technologies to perform passenger identification verification.

Sincerely,



Eddie D. Mayenschein
Assistant Administrator
Security Policy and Industry Engagement

Attachment



Transportation
Security
Administration

U.S. Department of Homeland Security
Transportation Security Administration
601 South 12th Street
Arlington, VA 20598

TSA-APPROVED SECURITY PROGRAM AMENDMENT

AIRCRAFT OPERATOR SkyWest Airlines (SWIA)

NUMBER SWIA-18-04

SUBJECT Biometric Identification Check – Checked Baggage Drop

PROGRAM 49 CFR 1544.101(a)

REFERENCE AOSSP Sections 4.2., 6.3., 6.4., 6.6., 7.2., 7.7.2., and 7.7.3.

LOCATION Atlanta Hartsfield-Jackson International Airport (ATL)

EFFECTIVE December 1, 2018

EXPIRES November 30, 2019

SUPERSEDES Not Applicable

PURPOSE AND GENERAL INFORMATION

This amendment allows the aircraft operator to use a bag drop system utilizing the Customs and Border Protection's (CBP) Traveler Verification Service (TVS) for passenger identification via facial recognition. The aircraft operator may accept and process checked baggage for flights departing from Atlanta Hartsfield-Jackson International Airport (ATL) without performing the passenger identification (ID) check and checked baggage acceptance measures as required in Sections 4.2., 6.3., 6.4., 6.6., 7.2., 7.7.2., and 7.7.3. of the Aircraft Operator Standard Security Program (AOSSP). This amendment is valid for one year while the Transportation Security Administration (TSA) evaluates the efficacy of these approved procedures under a proof of concept.

APPROVED PROCEDURES

A. TVS Performance Requirements

The aircraft operator must ensure:

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be released to persons without a "need to know" as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalties and other action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

~~SENSITIVE SECURITY INFORMATION~~

1. Biographic and biometric data collected by the TVS from participating passengers is maintained, transmitted, and disposed of in a manner which prevents unauthorized access and/or release of the information.
 2. The use of the TVS system, for purposes of providing services to the aircraft operator in connection with this proof of concept, meets or exceeds the information security standards specified and approved by TSA.
 3. The TVS matching thresholds meet or exceed the following:
 - a) True Match Rate of greater than or equal to 97 percent and;
 - b) False Match Rate/False Positive Identification Rate (FPIR) of less than or equal to 0.1 percent and;
 - c) False Non Match Rate (FNMR)/False Negative Identification Rate (FNIR) of less than or equal to 3 percent.
- B. The aircraft operator's assigned Principal Security Inspector (PSI) and ATL's Federal Security Director (FSD) or designee must be immediately notified in the event of program information being misplaced or compromised during collection, storage, transmission, or disposal.
- C. Passenger Biometric Bag Drop
1. The aircraft operator must comply with the following procedures in lieu of those contained in AOSSP Sections 4.2., 6.3., 6.4., 6.6., 7.2., 7.7.2., and 7.7.3. only when accepting checked baggage of passengers using valid government issued passports or visas verified by the TVS facial recognition system.
 2. Ensure that only passengers holding a valid passport or visa as identification with images stored in the TVS photo gallery use the facial recognition system and all other identification credentials undergo a manual check by a direct aircraft operator employee or authorized representative.
 3. Require all passengers using the TVS to undergo a biometric facial scan that will compare and match the facial scan of the passenger against the stored TVS database image of the passenger. The name of the passenger tendering the checked baggage to the direct employee or authorized representative must match the name appearing on the paper or mobile boarding pass and checked baggage destination tag(s) issued/printed in the Departure Control System.
 4. Prevent Inhibited Boarding Pass Printing Result (BPPR) passengers from using the TVS; and ensure they are referred to the aircraft operator's direct employee or authorized representative for a manual passenger identification check as described in AOSSP Section 4.2.

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be released to persons without a "need to know" as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalties or other action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

~~SENSITIVE SECURITY INFORMATION~~

the aircraft operator's TSA-approved security program, the aircraft operator must control accessibility and dissemination of this document in accordance with 49 CFR 1544.103(b).

- B. Changes to the AOSSP may require a corresponding revision of this amendment. It is the responsibility of the aircraft operator to review this amendment when a change to the AOSSP revises relevant requirements. Consult the assigned PSI or IIR, as appropriate, to determine if revision of this amendment is required.
- C. TSA may withdraw approval for use of this amendment without notice. Approval for use of this amendment expires at the end of the calendar day listed in the expiration date section above. The aircraft operator must submit a written request for renewal to the assigned PSI or IIR at least 45 calendar days prior to expiration.



David P. Pekoske
Administrator



Testing and Evaluation (T&E) Methodology for Automation of Passenger Identification and Bag Drop Operations

A. Introduction

This document defines the methodology for testing and evaluation of new automated biometric technology implementations of Customs and Border Protection’s (CBP) Traveler Verification Service (TVS). Aircraft Operators (AO) must demonstrate that the security effectiveness of the technology implementation is commensurate with or exceeds the requirements established by the Transportation Security Administration (TSA). Table 1 below lists the planning and execution steps for implementation of CBP’s TVS.

Table 1

Planning and Execution Steps
1. Draft & Submit T&E plan
2. Refine T&E plan with TSA guidance
3. Conduct testing for data collection
4. Report test results to TSA and request an amendment
5. Draft Quality Assurance (QA) plan based on Report finding
6. Report results and information specified in QA plan

B. Draft and Submit T&E Plan

AOs are responsible for designing an experiment to collect data that will demonstrate the efficacy of their technology solution. The experimental design will be communicated to TSA in a draft T&E plan. The draft plan defines the procedures and guidelines that AOs will employ to measure and report compliance with TSA requirements. The T&E plan to be drafted and submitted to TSA should clearly define the items in Table 2 below.

Table 2

Definition Required	Note
System components	System components performing identification (ID) verification requirements in relevant security programs, amendments, or Alternative Procedures (AP).
Experiment setup for laboratory evaluation and/or controlled operational pilot evaluation	Plan for providing ID verification measures that would allow for operations without an amendment providing relief from Section 4.2. of the AOSSP, if operational pilots are used for evaluation.

Methodology to collect required data to demonstrate adherence to requirements	Include: <ul style="list-style-type: none"> • Data collection time period • How data will be collected and verified • Duration of data collection • Number of data points' statistical justification for overall experiment design
Decision Points	Decision points to scale using a graduated approach to full operational scale based on result from laboratory testing and controlled operational pilots

C. TSA Requirements

1) Identity Verification Automation Requirements

The data reported to TSA will be used to assure that the automated ID check is functioning within the parameters established in this amendment, identify any potential issues, monitor configuration changes, and to provide TSA more insight into the operational functionality of the TVS service. The T&E plan submitted must address data collection and define a reporting strategy for the following.

- a. Traveler Types: Travelers are categorized with respect to how the scope of the program applies to them and three fundamental categories should be identified:
 - i. In-Scope: International Outbound Itinerary Traveler (>18 years old)
 - ii. Out-of-Scope: International Outbound Itinerary Travelers (<18 years old) and Domestic Itinerary Travelers
 - iii. Other: In-Scope Travelers without biometrics on file due to system issues, imposters, minors, other exceptions. Please note that some of these status indications are accessible through CBP-owned or operated data or system components.

- b. Match Performance: Two error metrics are used to quantify biometric matching performance for verification or identification of passengers:
 - i. True Match Rate (TMR) or True Positive Identification Rate (TPIR): This metric is calculated simply as the ratio of correct matches, i.e. matches in which the passenger was correctly identified, to the total number of matches:

$$TMR = \frac{\text{Correct matches}}{\text{Total matches}}$$

Note that False Non-Match Rate (FNMR) and False Negative Identification Rate (FNIR) are the inverses of TMR and TPIR, respectively.

- ii. False Match Rate (FMR) or False Positive Identification Rate (FPIR): This metric is the ratio of in-scope itinerary false matches, i.e. passengers that matched incorrectly against another, to the total number of matches:

$$FPIR = \frac{\text{In - scope itinerary false matches}}{\text{Total matches}}$$

These metrics are subject to two benchmarks. The threshold rate is the highest acceptable error rate or the lowest acceptable accuracy rate. The objective rate is the desired error or accuracy rate.

- c. Transaction Data: In addition to a cumulative summary, which provides the total number of matches (passenger transactions) alongside the two matching performance metrics, the following information, per transaction, is also desired, if available:

1. Timestamp of transaction
2. Unique Identifier (UID) return from TVS
3. Traveler Passenger Name Record (PNR), Passenger Record Locator (PRL)
4. Match Outcome (Hit/No Hit)

2) Data Confidence Requirements

Table 3 summarizes approximate data size options as they relate to confidence. Data provided during the initial implementation and evaluation period should be of STRONG or SUPERIOR confidence level. A MEDIUM confidence level is acceptable for data reported for expansions and other non-substantial changes.

Table 3

Option	Duration	Confidence Level	Transaction Count	Level of Effort
1: Small	less than a week	WEAK	<1,000	lowest
2: Medium	1 week	MEDIUM	btw 1,000 and 4,000	medium
3: Large	1 month	STRONG	btw 4,000 and 12,000	high
4: Very Large	Q (3 months)	SUPERIOR	>12,000	highest

We recommend more than a day's worth of data to be collected, and a continuous timeline that follows consecutive dates. If the collected samples are not independent, the specific issue causing the variance, to the extent that it can be identified, should be reported.

D. Refine T&E Plan with TSA Guidance

While drafting the test plan, AOs are encouraged to engage TSA for guidance. The objective of the AO/TSA engagement is to mitigate a guessing game in designing an experiment that will address TSA's information needs. TSA will work with AOs as a test plan is developed to provide clarity and to negotiate acceptable data collection strategies. The main goal is to generate quality data in a manner that is effective and efficient for AOs to execute.

E. Conduct Testing for Data Collection

Evaluations can be carried out in laboratory tests and/or controlled operational pilots to collect data while still performing manual procedures. During the testing phase, data should be provided and reviewed with TSA to assess the commensurate level of security effectiveness of the solution. If the evaluation approach being used is a phase approach, preliminary data and analysis will help expedite a decision of phasing out a manual procedure. In the case where a phased approach is not being implemented, preliminary data and analysis will also allow TSA to expedite the final review.

F. Report Test Results to TSA

Finalize a testing and evaluation report to TSA prior to issuance of the Biometric Identification Checked Baggage Drop amendment. The report should summarize:

- 1) Test approach
- 2) The experimental design
- 3) The solution configuration and final solution configuration
- 4) Data collection methods
- 5) Changes made throughout the testing phase
- 6) Final data analysis

The amendment will be approved, rejected, or conditionally approved based on the results of the evaluation.

G. Draft Quality Assurance plan

A draft Quality Assurance (QA) plan that defines the procedures and guidelines that AOs will employ to monitor, measure, and report compliance with TSA requirements upon

broader operations of the system. The QA plan also needs to articulate the appropriate configuration management that is in place by the AO and their service providers or vendors. The development of the QA plan will be similar to the development of the Test and Evaluation plan already discussed. The QA plan is intended to generate much of the same data that is delivered in the initial test and evaluation. The QA plan should leverage a solid experimental design that is minimally impactful to AO operations. TSA will work with AOs to help reach a mutually beneficial solution.

H. Quality Assurance Report

Submit QA and system performance data (i.e. every 6-12 months) to prove that the solution is meeting requirements in operations thereafter amendment approval.

~~SENSITIVE SECURITY INFORMATION~~

2. The use of the TVS system, for purposes of providing services to the aircraft operator in connection with this proof of concept, meets or exceeds the information security standards specified and approved by TSA.
 3. The TVS matching thresholds meet or exceed the following:
 - a) True Match Rate of greater than or equal to 97 percent and;
 - b) False Match Rate/False Positive Identification Rate (FPIR) of less than or equal to 0.1 percent and;
 - c) False Non Match Rate (FNMR)/False Negative Identification Rate (FNIR) of less than or equal to 3 percent.
- B. The aircraft operator's assigned Principal Security Inspector (PSI) and ATL's Federal Security Director (FSD) or designee must be immediately notified in the event of program information being misplaced or compromised during collection, storage, transmission, or disposal.
- C. Passenger Biometric Bag Drop
1. The aircraft operator must comply with the following procedures in lieu of those contained in AOSSP Sections 4.2., 6.3., 6.4., 6.6., 7.2., 7.7.2., and 7.7.3. only when accepting checked baggage of passengers using valid government issued passports or visas verified by the TVS facial recognition system.
 2. Ensure that only passengers holding a valid passport or visa as identification with images stored in the TVS photo gallery use the facial recognition system and all other identification credentials undergo a manual check by a direct aircraft operator employee or authorized representative.
 3. Require all passengers using the TVS to undergo a biometric facial scan that will compare and match the facial scan of the passenger against the stored TVS database image of the passenger. The name of the passenger tendering the checked baggage to the direct employee or authorized representative must match the name appearing on the paper or mobile boarding pass and checked baggage destination tag(s) issued/printed in the Departure Control System.
 4. Prevent Inhibited Boarding Pass Printing Result (BPPR) passengers from using the TVS; and ensure they are referred to the aircraft operator's direct employee or authorized representative for a manual passenger identification check as described in AOSSP Section 4.2.
 5. Require all (b)(3):49 U.S.C. § 114(r)
(b)(3):49 U.S.C. § 114(r)



Transportation
Security
Administration

U.S. Department of Homeland Security
Transportation Security Administration
601 South 12th Street
Arlington, VA 20598

TSA-APPROVED SECURITY PROGRAM AMENDMENT

AIRCRAFT OPERATOR Delta Air Lines (DALA)

NUMBER DALA-18-04

SUBJECT Biometric Identification Check – Checked Baggage Drop

PROGRAM 49 CFR 1544.101(a)

REFERENCE AOSSP Sections 4.2., 6.3., 6.4., 6.6., 7.2., 7.7.2., and 7.7.3.

LOCATION Atlanta Hartsfield-Jackson International Airport (ATL)

EFFECTIVE December 1, 2018

EXPIRES November 30, 2019

SUPERSEDES Not Applicable

PURPOSE AND GENERAL INFORMATION

This amendment allows the aircraft operator to use a bag drop system utilizing the Customs and Border Protection's (CBP) Traveler Verification Service (TVS) for passenger identification via facial recognition. The aircraft operator may accept and process checked baggage for flights departing from Atlanta Hartsfield-Jackson International Airport (ATL) without performing the passenger identification (ID) check and checked baggage acceptance measures as required in Sections 4.2., 6.3., 6.4., 6.6., 7.2., 7.7.2., and 7.7.3. of the Aircraft Operator Standard Security Program (AOSSP). This amendment is valid for one year while the Transportation Security Administration (TSA) evaluates the efficacy of these approved procedures under a proof of concept.

APPROVED PROCEDURES

A. TVS Performance Requirements

The aircraft operator must ensure:

1. Biographic and biometric data collected by the TVS from participating passengers is maintained, transmitted, and disposed of in a manner which prevents unauthorized access and/or release of the information.

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be released to persons without a "need to know" as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

~~SENSITIVE SECURITY INFORMATION~~

6. Direct passengers who fail the biometric match at the TVS to a direct employee or authorized representative for manual passenger identification check and checked baggage acceptance as described in AOSSP Section 4.2.
 7. Prevent the use of TVS by any passenger under 14 years of age traveling alone or with other travelers under the age of 14.
- D. Verbally notify the PSI and the ATL FSD or his designee within 24 hours of all TVS system data breaches, data losses or data exposure of biometric information.
- E. 6 months after the effective date of this amendment, the aircraft operator must submit to the PSI a diagnostic report detailing performance levels (including the False Positive Identification Rate – FPIR) of the baggage drop and specifics on collection, storage and transmission rates.
- F. Should the aircraft operator seek to change its provider of biometric identification services to one other than TVS, this amendment will be cancelled.
- G. DALA may use TVS as authorized by this amendment but the liability for compliance with all TSA requirements remains with DALA at all times.

SECURITY DIRECTIVES

When TSA issues a Security Directive (SD) requiring additional security measures, the aircraft operator must comply with any procedures concerning passenger identification and checked baggage acceptance. The aircraft operator must also inform its assigned Principal Security Inspector (PSI) or International Industry Representative (IIR), as appropriate, how it will implement such SD requirements.

SCOPE AND DURATION OF APPROVAL

- A. In accordance with title 49 of the Code of Federal Regulations (CFR), section 1544.105(b), this document amends the TSA-approved security program adopted by the aircraft operator in accordance with the requirements of 49 CFR 1544.101(a). As this amendment is part of the aircraft operator's TSA-approved security program, the aircraft operator must control accessibility and dissemination of this document in accordance with 49 CFR 1544.103(b).
- B. Changes to the AOSSP may require a corresponding revision of this amendment. It is the responsibility of the aircraft operator to review this amendment when a change to the AOSSP revises relevant requirements. Consult the assigned PSI or IIR, as appropriate, to determine if revision of this amendment is required.

~~Warning: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be released to persons without a "need to know" as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

- C. TSA may withdraw approval for use of this amendment without notice. Approval for use of this amendment expires at the end of the calendar day listed in the expiration date section above. The aircraft operator must submit a written request for renewal to the assigned PSI or IIR at least 45 calendar days prior to expiration.



David P. Pekoske
Administrator