

**STATEMENT OF RESPONSIBILITIES (SOR)
FOR
PARTICIPATION IN THE TRANSPORTATION SECURITY ADMINISTRATION'S
(TSA) AVIATION FEDERAL BUREAU OF INVESTIGATION (FBI) RECORD OF
ARRESTS AND PROSECUTIONS (RAP) BACK PROGRAM**

I. PURPOSE

The purpose of this SOR is to document the responsibilities, functions, and participation of the Airport/Aircraft Operator with respect to the TSA Aviation FBI Rap Back Program to implement recurrent criminal history records checks (CHRCs).

II. AUTHORITIES

TSA enters into this SOR under the provisions of 49 U.S.C. §§ 106(l)(6) and (m); 49 U.S.C. § 114(m)(1); and section 3405 of Pub. L. 114-190, 130 Stat. 615 (July 15, 2016).

III. SCOPE

The scope of this SOR includes:

The **Airport Operator or Aircraft Operator**, subject to TSA regulations, which is currently required to adjudicate the results of a fingerprint-based CHRC of certain individuals, and is a participating subscriber in FBI Rap Back.

IV. DEFINITIONS

Applicant: An individual who is applying for any ID media or privilege

Biometric Data: Data derived from the measurement of physiological or behavioral human characteristics used for the automated identification of individuals, including but not limited to fingerprints, palm prints, DNA, iris, and face.

Channeling Services: Services provided by a TSA-contracted Designated Aviation Channeling (DAC) that involve the collection and transmission of Personally Identifiable Information (PII) from regulated stakeholders to TSA for vetting purposes.

Classified Information: National security information that has been determined to require protection against unauthorized disclosure.

Confidential Information: When commercial or financial information is both customarily and actually treated as private by its owner and provided to the government under an assurance of privacy.

Rap Back Program SOR: TSA and Airport Operator or Aircraft Operator

Criminal History Records Check (CHRC): A search for an individual's criminal history by submitting the individual's fingerprints and biographic information to the FBI Criminal Justice Information Services (CJIS) Division's Next Generation Identification (NGI) system, and review of any criminal history records that NGI returns.

Criminal History Record Information (CHRI): See "Identity History Summary."

Current Media/Privilege Holder: An individual who holds airport issued media or privileges resulting from a CHRC.

Designated Aviation Channeler (DAC): A TSA contractor who is under Agreement with TSA to provide channeling services to the nation's airport and aircraft operators. There are currently two DACs: American Association of Airport Executives (AAAE) and Telos ID.

Electronic Biometric Transmission Specification (EBTS): Requirements to which agencies must adhere when electronically communicating with the FBI as they relate to the electronic encoding and transmission of biometric image, biographic information, and arrest data. The most current requirements are posted on the FBI website at www.fbibiospecs.cjis.gov.

Identity History Summary (IdHS) (also known as a "rap sheet"): The report of all identification, demographic, and event information, criminal and/or civil, within an FBI Next NGI Identity record that may be disseminated to an authorized recipient.

Next Generation Identification (NGI) System: Replacement for the FBI's Integrated Automated Fingerprint Identification System (IAFIS) that provides new functionality and improves upon existing capabilities, in particular for criminal history records search functions.

Personally Identifiable Information (PII): Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

FBI Rap Back: A service provided by the FBI that enables authorized entities the ability to receive on-going status notifications of any identity history changes reported to the FBI on individuals holding positions of public trust, such as those positions required by TSA to complete a CHRC.

Privileged Information: Information that involves the government deliberative process or involves the attorney-work product or attorney-client communications.

Proprietary Information: Information (also known as a trade secret) that a company wishes to keep confidential such as secret formulas, processes, and methods used in production.

Rap Back Activity Notification (RBN): Unsolicited notification received from the FBI that there has been new reported activity on a subscribed person's IdHS.

Sensitive But Unclassified Information: Information that is designated as sensitive to control and to which access is restricted because its release could cause harm to a person's privacy or

Rap Back Program SOR: TSA and Airport Operator or Aircraft Operator

welfare, adversely impact economic or industrial institutions, or compromise programs or operations essential to the safeguarding the national interests.

Sensitive Security Information (SSI): SSI is information obtained in the conduct of security activities whose public disclosure would be detrimental to transportation security, be an unwarranted invasion of privacy, or reveal trade secrets or privileged or confidential information. See 49 Code of Federal Regulations (CFR) 1520.5.

Submitting Entity: An authorized Federal agency, such as TSA, that submits fingerprints to the FBI for background searches and Rap Back subscriptions.

Subscribing Entity: Entities (such as an aircraft operator, and/or an airport operator) authorized under statute, executive order, or regulation to receive IdHS and who are subscribing individuals to the FBI's Rap Back Service.

Subscription: Term used to describe the agreement between the FBI and an entity in which the FBI provides notice of any future criminal data received on an individual for whom the entity submitted fingerprints and a Rap Back subscription request to the FBI.

Subscription Management Plan: An FBI required plan to define how the Submitting Entity will manage the subscriptions they submit to NGI.

V. ROLES AND RESPONSIBILITIES

A. Airport Operator or Aircraft Operator must:

- 1) Collect and/or transmit biometrics (fingerprints) that meet the most recent FBI EBTS specifications, minimum version 10.0, supported by the DAC;
- 2) Provide an updated Privacy Act Statement, 5 U.S.C. 552a(e)(3), (issued as attachment to the 1542-04-08 series Security Directives), to each applicant when he or she provides fingerprints for the required CHRC;
- 3) Review all IdHS information returned, determine if a disqualifying arrest or offense has occurred, take appropriate action based on that determination in accordance with 49 CFR 1542.209 and 1544.209, and annotate TSA's system with the action taken, as applicable;
- 4) Ensure that resources are available to support the timely adjudication of an updated IdHS resulting from an RBN, a subsequent Rap Back subscription, a consolidation notice, a Rap Back IdHS request response and all Rap Back subscription maintenance transactions;
- 5) Review or confirm validation of Rap Back subscription expiration date(s) to badge expiration dates, and provide updates to TSA including expired or canceled records on a monthly basis as needed for Rap Back subscriptions, supported by the DAC;

Rap Back Program SOR: **TSA and Airport Operator or Aircraft Operator**

- 6) Review initial data transmission to ensure that all submitted subscriptions are captured in the FBI system and the system used by the Participant, supported by the DAC;
- 7) Provide an automated method to submit subscriptions to TSA for transmission to FBI for each individual enrolled in Rap Back via TSA-approved method(s), supported by the DAC;
- 8) Send a transaction to TSA to update an applicant or current media/privilege holder's record of change in credential/benefit status (e.g., revoked, not issued, issued, etc.), supported by the DAC;
- 9) Send a transaction to TSA to update an applicant or current media/privilege holder's record, upon confirmation by the applicant or current media/privilege holder of an alias, if the IdHS reflects an undisclosed alias, supported by the DAC;
- 10) Provide timely submission of subscription entry to TSA for transmission to the FBI, supported by the DAC;
- 11) Provide timely submission of subscription cancellations to TSA for transmission to the FBI to remove the subscription from the Rap Back Service, supported by the DAC;
- 12) Provide timely submission of subscription modifications to TSA for transmission to the FBI, supported by DAC;
- 13) Assume all costs to support additional RBN review and airport operator/aircraft operator adjudication workflow, and other FBI Rap Back subscription management requirements that are necessary;
- 14) Maintain and update applicant credential/benefit status through the DAC as required by the most current applicable TSA Security Directive, supported by the DAC;
- 15) Follow the work flow established by TSA for setting up FBI subscriptions, supported by the DAC;
- 16) Follow Rap Back subscription maintenance procedures defined by the FBI and TSA, supported by the DAC; and
- 17) Address all errors received from the FBI or TSA and take the necessary actions to correct submissions, supported by the DAC.

B. TSA will:

- 1) Serve as the single point of contact between the FBI and airport/aircraft operators for Rap Back subscription submissions, subscription maintenance transactions and Rap Back Activity Notifications;

Rap Back Program SOR: **TSA and Airport Operator or Aircraft Operator**

- 2) Receive and transmit biometrics (fingerprints) meeting the most recent FBI EBTS specifications minimum version 10.0 to FBI;
- 3) Establish written guidance/maintenance procedures to support the Rap Back subscription process in accordance with FBI guidance;
- 4) Provide training to Participants to meet FBI privacy mitigation and subscription management requirements;
- 5) Provide training to Participants on updated Privacy Act Statement, authority to access Criminal History Record Information (CHRI), subscription submission, maintenance transaction submission, receipt of Rap Back Activity Notifications and setting of subscription expiration dates;
- 6) Develop a Privacy Risk Mitigation Strategy according to FBI requirements, and provide to Participants;
- 7) Provide Participant training to ensure that CHRC and Rap Back subscription packages meet TSA requirements including Full package (FP) vs Fingerprint Only (FPO) and Previously Fingerprinted (PFP);
- 8) Facilitate the Rap Back service between Participants and the FBI;
- 9) Transmit conforming biometrics (fingerprints) received from Participants to the FBI;
- 10) Develop and provide a Subscription Management Plan (include set-up, modify, extend, delete, and synchronize subscriptions) for Participants;
- 11) Receive subscription updates from Participants and transmit this information to the FBI;
- 12) Accept an RBN from the FBI subsequent to an initial CHRC response;
- 13) Determine which triggering events will be set for an RBN;
- 14) Select the format of future RBNs;
- 15) Receive a Rap Back subscription renewals list from the FBI and transmit this information to the Participant;
- 16) Receive a transaction from Participants to update the applicant's record of change in credential/benefit status (e.g., revoked, not issued, issued, etc.) for an applicant;
- 17) Follow the designated work flow for setting up FBI Rap Back subscriptions;
- 18) Choose an appropriate Privacy Risk Mitigation Strategy for the Rap Back subscriptions in accordance with FBI requirements;

Rap Back Program SOR: TSA and Airport Operator or Aircraft Operator

19) Notify FBI of records that should be removed (cancelled) from the Rap Back subscription list at the expiration of the badge or end of subscription term, as provided from Participants.

VI. HANDLING, SHARING, AND PROTECTION OF INFORMATION

- A. The airport/aircraft operator must take appropriate measures to protect proprietary, privileged, confidential, personally identifiable information (PII), or otherwise Sensitive Security Information (SSI) that it may observe, control, or possess.
- B. The Parties agree that subsequent uses and treatment of information shared under this SOR must be afforded protection from disclosure to third parties to the extent permissible under the Freedom of Information Act, 5 U.S.C. § 552, subject to disclosure restrictions contained in the Privacy Act (PA), 5 U.S.C. § 552a, Sensitive Security Information, 49 CFR part 1520, and any other applicable laws.
- C. The Airport/Aircraft Operator acknowledges that all records and data must be handled in accordance with the requirements for handling Sensitive Security Information (SSI) under 49 U.S.C. § 114(r) and 49 C.F.R. part 1520. All members assigned to work under this Agreement are subject to the provisions of 49 CFR part 1520, Protection of Sensitive Security Information, because they act for, or carry out duties for, or act on behalf of TSA. All Parties will have access to the current guidelines for handling SSI and to any updates made in the future.
- D. The Airport/Aircraft Operator must take appropriate measures to protect proprietary, privileged, Classified, and Sensitive but Unclassified information that may come into their possession as a result or in furtherance of this SOR. Nothing shall limit TSA's ability to share information within DHS to those components/employees that have a "need to know" the information in the performance of their official duties.
- E. To prevent the unauthorized disclosure, copying, use, or modification of information provided under this SOR, the Parties must restrict access to such information on a need to know basis and use recognized security mechanisms such as passwords, encryption, or other reasonable safeguards to prevent unauthorized access.
- F. Prior to releasing any information to the media regarding any prosecution, investigation, or other enforcement action based on information developed under this SOR, the Parties must confer and release with TSA approval in order to ensure that the information to be released is accurate and may otherwise be properly disclosed. The release of any PII to the media must be in compliance with the applicable PA System of Records.
- G. No SSI, oral or written, concerning the scope of this Agreement, shall be published or released to the public, without prior written approval of the TSA Administrator or his designee.

Rap Back Program SOR: **TSA and Airport Operator or Aircraft Operator**

H. The sharing of information between the Parties must be conducted under applicable law. The Parties must appropriately safeguard information shared in accordance with the PA, applicable laws, regulations, executive orders, policies and procedures; the Attorney General guidelines; and policies and procedures of the TSA, and the Department of Homeland Security.

VII. ADMINISTRATION

A. Administration and compliance with the provisions of this SOR are the responsibility of Airport/Aircraft Operator. The Airport/Aircraft Operator must appoint a representative to act as the Point of Contact (POC) for routine administration, management, operational, and other matters associated with this agreement.

B. The Airport/Aircraft Operator POCs:

For routine administrative matters:
Name: Michael Parks, Airport Manager
Email: Michael.Parks@como.gov
Phone: 573-817-5064

For operational matters:
Name: Michael Parks
Email: Michael.Parks@como.gov
Phone: 573-817-5064

SIGNATORY AUTHORITY:

The undersigned represent that they have the authority to bind and/or otherwise commit their respective organizations to the terms, conditions, duties and responsibilities contained in this SOR.

Leadership Name
Title
Organization



Approved as to form:

City Counselor



Date

Rap Back Program SOR: TSA and Airport Operator or Aircraft Operator