

Department of Homeland Security
Office of Inspector General

**Use of Risk Assessment within
Secure Flight**

(Redacted)





OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

July 6, 2015

MEMORANDUM FOR: The Honorable Peter Neffenger
Administrator
Transportation Security Administration

FROM: John Roth *John Roth*
Inspector General

SUBJECT: *Use of Risk Assessment within Secure Flight –
Redacted*, OIG-14-153
OSC File No. DI-14-3012

Attached for your information is the redacted version of our Sensitive Security Information (SSI) final letter report: *Use of Risk Assessment within Secure Flight*. We issued the SSI version of this report to the Department on September 9, 2014, and closed Recommendation 2 because of the Transportation Security Administration's (TSA) corrective actions to address the intent of this recommendation.

After issuing the report, TSA has implemented additional plans and taken corrective actions to address the remaining report recommendations. Based on TSA's responses, Recommendations 1 and 3 are currently resolved and open.

We coordinated a sensitivity review of the SSI final letter report with TSA and have reached agreement on the appropriate redactions. We are now making the redacted report public and will publish it on our website.

Please call me with any questions, or your staff may contact Anne L. Richards, Assistant Inspector General for Inspections, at (202) 254-4100.

Attachment




SENSITIVE SECURITY INFORMATION

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

SEP 09 2014

MEMORANDUM FOR: The Honorable John S. Pistole
Administrator
Transportation Security Administration

FROM: John Roth 
Inspector General

SUBJECT: *Use of Risk Assessment within Secure Flight – Sensitive Security Information*
OSC File No. DI-14-2012

Attached for your information is our final letter report, *Use of Risk Assessment within Secure Flight – Sensitive Security Information*. This report is in accordance with the requirements of 5 U.S.C. § 1213(d). We incorporated formal comments from the Transportation Security Administration (TSA) in the final report.

The report contains three recommendations aimed at improving TSA Pre✓™ Initiative security. Your office concurred with one recommendation and did not concur with two. Based on information provided in your response, we consider Recommendation 1 resolved and open, Recommendation 2 resolved and closed, and Recommendation 3 unresolved and open. No further reporting is necessary for Recommendation 2.

Within 90 days of the date of this memorandum, please provide our office with a written response that includes your (1) corrective action plan and (2) target completion date for each recommendation. Also, please include responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendation.

We are providing a copy of this report to the Department of Homeland Security's General Counsel. We are not releasing this report publicly because of its sensitivity.

SENSITIVE SECURITY 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 disclosed 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~~

OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

Major contributors to this report are Marcia Moxey Hodges, Chief Inspector; Angela Garvin, Lead Inspector; Amy Tomlinson, Senior Inspector; LaDana Crowell, Senior Inspector; and Rahne Jones, Inspector.

Please call me with any questions, or your staff may contact Deborah L. Outten-Mills, Acting Assistant Inspector General, Office of Inspections, at (202) 245-4015

cc: The Honorable Stevan E. Bunnell
General Counsel

Attachment

~~SENSITIVE SECURITY 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 disclosed 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.~~



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

Review Request

The U.S. Office of Special Counsel (OSC) received a whistleblower disclosure concerning the use of a risk-based rule by the Transportation Security Administration’s (TSA) Secure Flight program that may create a vulnerability in aviation security. The risk-based rule

[REDACTED]. The disclosure also stated the Secure Flight program [REDACTED]. On April 28, 2014, OSC referred this allegation to the Secretary of Department of Homeland Security. The Department subsequently requested our assistance with this allegation.

Conduct of Review and Summary of Evidence Obtained

We assigned our Office of Inspections team currently assessing Security Enhancements to the TSA Pre✓™ Initiative to review this allegation. We interviewed the whistleblower and TSA senior officials involved in the risk-based rule decision-making process. We also analyzed documentation regarding these rules to determine whether an aviation security vulnerability exists.

We analyzed the following [REDACTED] documents:

- Memoranda establishing the rule;
- Memorandum suspending the rule;
- TSA Office of Security Operations’ evaluation of the rule; and
- Secure Flight program documentation evidencing rule status.

Summary of Results

We determined that [REDACTED] using risk-based analysis by TSA’s Secure Flight Program [REDACTED]. However, TSA mitigated the risk on March 7, 2014, by suspending the rule’s use in the Secure Flight program. We recommend TSA discontinue using the rule until TSA [REDACTED].



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

Secure Flight Screening

TSA's Secure Flight program screens individuals prior to granting them access to an airport's sterile area. The program allows TSA to determine the level of security screening passengers should receive at the airport checkpoint. The program compares self-reported traveler information provided to TSA from air carrier reservations, such as name, date of birth, and gender, to lists of low-risk travelers, the Terrorist Screening Database No Fly and Selectee Lists, as well as to other intelligence-based data systems maintained by TSA and other Federal agencies.

Risk Assessment Rule [REDACTED]

[REDACTED]

[REDACTED]¹ TSA Pre✓™ screening generally involves the use of a walkthrough metal detector. Passengers are not required to remove shoes, belts, laptops, liquids, or gels. The equipment used to screen carry-on baggage contains threat-recognition software that aids the Transportation Security Officer's review of this baggage. As a result, the carry-on baggage belt runs continuously rather than stopping at each bag. However, the Transportation Security Officer has the ability to stop the belt when needed.

[REDACTED]

¹ [REDACTED]



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov



Source: OIG Analysis of TSA Data.

These passengers can then print boarding passes with the TSA Pre[✓]™ indicator. [REDACTED]

[REDACTED]

TSA Leadership is Aware of [REDACTED]

Prior to implementing the Secure Flight risk assessment rules, TSA leadership acknowledged [REDACTED]. TSA officials considered that a terrorist operative, [REDACTED]. [REDACTED]



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

[REDACTED]

TSA Suspend the Secure Flight Risk Assessment [REDACTED]

Following rule implementation, TSA officials received complaints [REDACTED]
[REDACTED]
[REDACTED] the Assistant Administrator for the TSA Office of Security Operations requested a 30-day suspension of the Secure Flight risk assessment rule for these passengers to assess the effect on [REDACTED]. TSA leadership said they suspended the rule because of operational efficiency challenges [REDACTED]. On March 7, 2014, Secure Flight removed this rule from the risk assessment rules. Since suspension, [REDACTED]
[REDACTED]
[REDACTED].

TSA is Developing Technology to Mitigate [REDACTED]

To mitigate [REDACTED] TSA is acquiring Credential Authentication Technology (CAT) that will be capable of verifying passenger data. TSA plans to conduct CAT operational testing in the first and second quarters of calendar year 2015. CAT deployment will be a phased approach. When first released, CAT machines will have identity document authentication technology with the automated ability to detect fraudulent identity documents. In the second phase, CAT will have Secure Flight connectivity to verify that passenger identity documents match the information vetted by Secure Flight during the flight reservation process.
[REDACTED]
[REDACTED]
[REDACTED]

While the recommended rule suspension timeframe has passed, we have not received documentation that TSA reinstated the rule. Interviews with TSA senior leadership



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

provided varied perspectives on the rule's future use. On June 27, 2014, we received a telephone call notifying us that TSA reinstated the rule. According to TSA officials, the rule's activation from June 18 to 24, 2014, was a mistake resulting from Secure Flight program updates. These officials also said upon discovery TSA corrected the mistake. In addition, our last correspondence on July 14, 2014, with Secure Flight Program officials indicates TSA has not instructed program officials to reinstate the rule.

We are making three recommendations to address this [REDACTED]
[REDACTED]

Recommendations

We recommend that the TSA Assistant Administrator for the Office of Security Capabilities:

Recommendation 1:

Explore the feasibility of encrypting commercial aircraft carrier boarding passes [REDACTED]
[REDACTED].

Recommendation 2:

Continue pursuing Credential Authentication Technology [REDACTED]
[REDACTED].

We recommend that the TSA Chief Risk Officer:

Recommendation 3:

Ensure Credential Authentication Technology is fully functional [REDACTED]
[REDACTED]
[REDACTED].

Management Comments and OIG Analysis



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

We evaluated TSA's written comments and made changes to the report where we deemed appropriate. A summary of TSA's written response to the report recommendations and our analysis of the response follows. A copy of TSA's response, in its entirety, is included as appendix A. In addition, we received technical comments from TSA and incorporated these comments into the report where appropriate. TSA concurred with one recommendation and did not concur with two. We appreciate TSA's comments and contributions.

Management Response to Recommendation #1: TSA officials did not concur with Recommendation 1. In its response, TSA said in 2012 it explored the cost and feasibility of encrypting commercial aircraft carrier boarding passes [REDACTED]. After engaging industry stakeholders, TSA decided not to adopt this approach because of limited data fields in some air carrier systems and encrypting boarding pass barcodes is cost prohibitive. TSA said it decided to pursue a more practical and affordable solution using a digital signature.

OIG Analysis: Although TSA did not concur with this recommendation, we consider TSA's actions responsive to the intent of Recommendation 1, which is resolved and open. We acknowledge TSA's previous efforts to encrypt boarding passes [REDACTED]. This recommendation will remain open pending our receipt of CAT Phase I and II timeframes, milestones, and implementation dates.

Management Response to Recommendation #2: TSA officials concurred with Recommendation 2. TSA said it is pursuing CAT and awarded a contract in April 2014 to begin operational testing and evaluation of this technology.

OIG Analysis: We consider TSA's actions responsive to the intent of Recommendation 2, which is resolved and closed. No further reporting from TSA regarding this recommendation is necessary.

Management Response to Recommendation #3: TSA officials did not concur with Recommendation 3. TSA said it mitigates the current level of risk [REDACTED] by a range of security procedures and technologies currently available and/or deployed by TSA.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

OIG Analysis: We consider TSA's actions nonresponsive to the intent of Recommendation 3, which is unresolved and open. Although TSA has developed tools and processes as security layers, these measures are not available at all airports. For example, as of June 2014 [REDACTED]. In addition, TSA Pre[✓]™ lanes use walkthrough metal detectors for passenger screening, but this technology does not detect non-metallic items. Advanced Imaging Technology machines identify and display metallic and non-metallic items and potential anomalies concealed on a passenger, affording Transportation Security Officers enhanced capabilities to screen passengers and identify threat items. Using walkthrough metal detectors in TSA Pre[✓]™ lanes limits TSA's security threat detection capabilities.

Further, [REDACTED] need improvement. [REDACTED]

Recommendation 3 will remain unresolved and open pending our receipt of documentation that [REDACTED] until CAT [REDACTED] Implementation.



Appendix A Management Comments to the Draft Report

SENSITIVE SECURITY INFORMATION

U.S. Department of Homeland Security
601 South 12th Street
Arlington, VA 22204

AUG 27 2014



Transportation
Security
Administration

INFORMATION

MEMORANDUM FOR: John Roth
Inspector General
U.S. Department of Homeland Security (DHS)

FROM: John S. Pistole
Administrator *John S. Pistole*

SUBJECT: Transportation Security Administration's Response to
DHS Office of the Inspector General (OIG) Draft Letter
Report, [REDACTED]
[REDACTED]
-
Sensitive Security Information (OSC File No. DI-14-
2012)

Purpose

This memorandum constitutes the Transportation Security Administration's (TSA) response to the DHS Office of the Inspector General (OIG) draft letter report, [REDACTED]
[REDACTED] - *Sensitive Security Information*, dated July 21, 2014.

Background

The U.S. Office of Special Counsel (OSC) received a whistleblower disclosure concerning the use of a risk-based rule by the Transportation Security Administration's (TSA) Secure Flight program. On April 28, 2014, OSC referred this allegation to the Secretary of the U.S. Department of Homeland Security. The Department subsequently requested the assistance of DHS OIG to review this allegation. OIG interviewed the whistleblower and TSA senior officials involved in the risk-based rule decision-making process. OIG also analyzed documentation regarding these rules to determine whether an aviation security gap exists.

OIG determined that [REDACTED]
[REDACTED]

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed 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.

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed 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.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

Discussion

TSA takes whistleblower disclosures seriously and appreciates the work of the OIG during this review. TSA will use the information to assist in our ongoing efforts toward effective Risk-Based Security.¹

TSA uses a variety of procedures and technologies to respond to the Agency's need to reduce transportation security vulnerabilities. Our decisions on the use of these tools, and on calibrating their rates, enable TSA to manage risk to achieve our security responsibilities while promoting the freedom of legitimate movement for people and commerce. One of the tools that we use as part of a layered security approach [REDACTED] through which TSA assigns a level of risk [REDACTED]. The current level of risk associated with [REDACTED] is mitigated by a range of security procedures and technologies currently available and/or deployed by TSA. In addition, the underlying analysis supporting [REDACTED] was independently assessed and deemed an effective means of evaluating low-risk passengers. Moreover, the determination about whether and how to employ [REDACTED] as part of a risk-based security approach to screening lies within the broad statutory authority granted the Administrator under 49 U.S.C. § 114 to consider intelligence, assess risk, and implement screening decisions consistent with the Agency's mission. Finally, in the 9/11 Act, Congress made clear that TSA needed to direct limited resources to providing the best security value and that the Agency had to establish risk-based priorities. The rule is consistent with this statutory mandate.

This rule is the focus of a whistleblower disclosure and related report, [REDACTED] - Sensitive Security Information. (OSC File No. DI-14-2012).

RISK ASSESSMENTS

In 2011, TSA began using modified screening procedures for passengers [REDACTED]

¹ TSA has broad ranging authority under 49 U.S.C. § 114, among other statutes, to consider intelligence, assess risk, and implement screening decisions consistent with the Agency's mission. See, e.g., 49 U.S.C. § 114(d) (1) and (2) (TSA is responsible for security in all modes of transportation that are exercised by the Department of Transportation); and 49 U.S.C. § 114(f) (1), (2) and (5) (TSA is mandated to distribute intelligence information related to transportation security, assess threats to transportation, and serve as the primary liaison for transportation security to the intelligence and law enforcement communities).

[REDACTED]

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed 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.

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed 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.~~



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

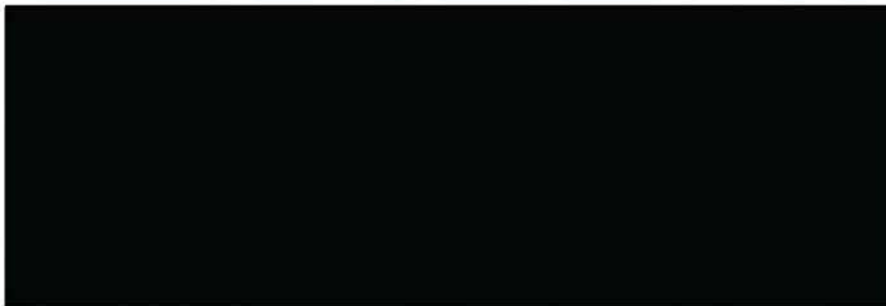
Washington, DC 20528 / www.oig.dhs.gov

SENSITIVE SECURITY INFORMATION

3

In October 2013, TSA implemented [REDACTED] criteria for identifying lower-risk passengers under the Secure Flight risk-based analysis initiative.³ This policy decision followed significant analysis of [REDACTED] of lower-risk travelers. In addition to TSA's internal analysis, [REDACTED] was assessed independently by Metron, Inc.⁴ Following [REDACTED] the Secure Flight pre-screening system, additional independent analysis [REDACTED] conducted by the Civil Aviation Threat Working Group (CATWG)⁵ and the Homeland Security Studies and Analysis Institute (HSSAI)⁶ which [REDACTED] separately and in conjunction with the two other risk assessment elements planned for implementation as part of Secure Flight risk-based analysis. During their assessment, CATWG analysts determined [REDACTED]

[REDACTED] The HSSAI assessment concluded that the approach TSA had taken in developing and implementing [REDACTED] based risk assessments was defensible.



Prior to implementing Secure Flight risk-based analysis, TSA used SFPD information to conduct automated checks against terrorist watch lists and as part of intelligence-based rules used to

³ See TSA's discussion of this initiative in its Privacy Act system of records notice (SORN), *Privacy Act of 1974; Department of Homeland Security Transportation Security Administration-DHS/TSA-019 Secure Flight Records System of Records*, 78 Fed. Reg. 55270 (Sept. 10, 2013).

⁴ Metron, Inc. is a scientific consulting company under contract to the DHS Office of Science and Technology that develops and applies mathematical methods for solving challenging problems in national defense and homeland security.

⁵ The CATWG is comprised of intelligence analysts from DHS and 10 other Intelligence Community agencies with expertise in civil aviation, and is chaired by a senior analyst from the National Counterterrorism Center (NCTC). Directly contributing to the results of the analysis were analysts from the Central Intelligence Agency, Federal Bureau of Investigation, NCTC, Federal Aviation Administration, and National Security Agency.

⁶ HSSAI is a Federally Funded Research and Development Center (FFRDC) created to provide independent analysis of homeland security issues for the U.S. Department of Homeland Security, its components and agencies, and its partner organizations, as authorized in the Homeland Security Act of 2002 (Pub. Law 107-296, § 305 as codified in 6 U.S.C. § 185).

⁷ Merit scores reflect the accuracy of classification on a scale from 0.0 to 1.0, where 1.0 reflects perfect classification, 0.5 reflects the expected results from random classification, and a value of 0.0 indicating misclassification of passengers by high or low risk.

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed 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.

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed 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.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

SENSITIVE SECURITY INFORMATION

4

identify potentially high-risk passenger. TSA now uses this information [redacted] to identify lower-risk travelers. These criteria, and the associated inclusion rates,⁸ must be viewed within the context of TSA's overall risk-based security approach and terrorist threats targeting commercial aviation.

Five key points of context are important to consider with respect to TSA's use of [redacted] criteria to identify lower-risk travelers.

1. **Intelligence.** Since the 9/11 terrorist attacks, the intelligence community has transformed its capability to collect, analyze, and share terrorist intelligence information. TSA has direct access to aviation-related intelligence information that has fundamentally improved our internal analytical capability.
2. **Global Partners.** TSA works globally with public and private partners, including foreign government, to improve the overall posture of aviation security.
3. **Pre-Screening.** Implementation of Secure Flight has automated matching against terrorist watch lists, known traveler lists, and other security-related data; and improved matching algorithms within Secure Flight has significantly reduced the percent of travelers who are incorrectly identified as being on a watch list. In addition, Secure Flight supports the application of intelligence-based [redacted] rules capability to better identify travelers who either may pose a higher threat to aviation security, or who may present a low risk to security. These capabilities provide TSA with 72-hour advance notice of Known or Suspected Terrorist (KST) travel and allow for adjustments to security measures to mitigate this elevated threat.
4. **Detection.** Improved detection capabilities now include advanced technology dual-view x-ray equipment, advanced imaging technology (AIT) equipment capable of detecting improvised explosive devices hidden beneath clothing, passenger screening canine team, improved explosives trace detection equipment, and a behavior detection program.
5. **Random and Covert.** TSA provides random Playbook activities at checkpoint, departure gates, and other areas of the airports. Our Federal Air Marshals (FAMs) [redacted]. In addition, all travelers, including known travelers, are subject to random screening to ensure unpredictable results, e.g. a traveler who might otherwise be eligible for expedited screening is provided standard screening.

At present, intelligence information continues to identify threats to commercial aviation originating in foreign countries and involving attacks with improvised explosive devices hidden either on the passenger or concealed in seemingly innocuous items commonly carried by travelers. [redacted]

Travelers eligible for expedited screening (eligibility [redacted])

[redacted]

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed 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.

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed 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.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

SENSITIVE SECURITY INFORMATION

5

printed on the traveler's boarding pass and embedded in the boarding pass barcode) have already been checked against all high-risk criteria, including: the No-Fly list, Selectee, and e-Selectee watch lists from the Terrorist Screening Center's (TSC's) Terrorist Screening Data Base (TSDB); intelligence-based high-risk rules; [REDACTED]; and the Do-Not-Board list maintained in conjunction with the Centers for Disease Control and Prevention (CDC). Following verification of their biographic and travel information against these high risk populations, passengers are then checked against low-risk populations using a known traveler number submitted with their airline reservation. Only travelers who have not matched against these previous checks are then considered for designation as low-risk travelers [REDACTED], and only if they have not been disqualified for participation in TSA Pre✓™ stemming from a violation of TSA security rules.

Passengers designated as TSA Pre✓™ eligible [REDACTED] are still subject to physical screening measures including a combination of randomly applied and required measures. Required physical screening measures include inspection and verification of travel documents (identification and boarding pass), x-ray inspection of all accessible property, and individual screening, in most cases through a walk-through metal detector (WTMD).⁹

Travelers designated for expedited screening may be subjected to random security measures that include Behavior Detection Observation, explosives trace detection, explosives detection canine teams, and AIT at checkpoints where available. Additional random security measures are also employed at departure gates and other areas of the airport. As noted in the August 8, 2013, Action Memorandum (attached), the technologies and screening procedures for passengers designated for expedited screening far exceed international standards used for general aviation security.

[REDACTED] As explained in the decision memorandum approving implementation [REDACTED], TSA considered the [REDACTED] a series of potential mitigation options, the potential that a terrorist operative might [REDACTED] [REDACTED] identified during Secure Flight pre-screening. However, in light of the totality of risk, TSA does not concur with the contention [REDACTED] that warrants immediate action.

⁹ AIT equipment is available for use at some TSA Pre✓™ screening checkpoints and is requested as a preferred physical screening method by some passengers with surgical implants that would cause the WTMD to alarm.

¹⁰ ACTION MEMORANDUM: from Victoria Newhouse and Kelly Hoggan, to John S. Pistole, TSA Pre✓™ [REDACTED] 8, 2013, pp. 3 – 4

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed 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.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

~~SENSITIVE SECURITY INFORMATION~~

6

Through the development and application of risk-based security principles, TSA has focused on developing effective and sustainable risk mitigation and risk management solutions to ensure our security measures are effective, flexible, sustainable, and focused on preventing catastrophic terrorist acts. Prior one-size-fits-all security measures concentrating on identifying certain high-risk passengers, finding dangerous objects, and otherwise attempting to eliminate risk are simply not sustainable and fail to provide the best security value to the American people.

An important part of providing the best security value to the American people is to identify low-risk airline passengers so that TSA may better focus its limited security resources on passengers who are more likely to pose a threat to civil aviation.¹¹ The notion of identifying low-risk aviation passengers so that screening resources can be directed to higher-risk passengers predates the creation of the TSA. In 1997, the White House Commission on Aviation Safety and Security recommended that the Federal Aviation Administration (FAA) work with airlines to support the development and implementation of nascent automated passenger screening systems that separate passengers "into a very large majority who present little or no risk, and a small minority who merit additional attention."¹²

After creation of TSA, Congress and others have continued the theme of directing the Agency to allocate scarce resources to provide the best security value. For example, in its final report, the National Commission on Terrorist Attacks Upon the United States (the 9/11 Commission) recommended that:

"Hard choices must be made in allocating limited resources. The U.S. Government should identify and evaluate the transportation assets that need to be protected, set risk-based priorities for defending them, select the most practical and cost-effective ways of doing so, and then develop a plan, budget, and funding to implement the effort. . . . In measuring effectiveness, perfection is unattainable. But terrorist should perceive that potential targets are defended. They may be deterred by a significant chance of failure."¹³

As directed by the 9-11 Commission and the Congress, TSA in fact is making hard choices to provide the most transportation security using the resources available. These choices include identifying low-risk passengers so more effort can be directed to high-risk passengers or those

¹¹ See the corresponding discussion in the SORN that announced the TSA Pre✓™ Application Program, *Privacy Act of 1974; Department of Homeland Security/Transportation Security Administration—DHS/TSA-021 TSA Pre✓™ Application Program System of Records*, 78 Fed. Reg. 55274 (Sept. 10, 2013). Under that program, individuals submit personal data to TSA, which conducts a security threat assessment. Applicants who meet the standards of the assessment are issued a Known Traveler Number for use when traveling. Passengers with KTNs typically receive expedited screening at airports with TSA Pre✓™ expedited screening lanes.

¹² White House Commission on Aviation Safety and Security, Final Report to President Clinton, sec. 3.19 (Feb. 12, 1997), found at www.fas.org/irp/threat/212fin-1.html.

¹³ See Final Report of the National Commission on Terrorist Attacks Upon the United States," page 391 (July 22, 2004).

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed 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~~

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed 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~~

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

~~SENSITIVE SECURITY INFORMATION~~

7

for whom risk is unknown. As noted by the 9-11 Commission, perfection is unattainable; however, a broad-based, sustained effort may deter terrorists.

Congress has solidly supported TSA's efforts to identify low-risk travelers for expedited screening in annual appropriations bills and in its oversight of TSA efforts in this regard. For example, in its report on the proposed fiscal year (FY) 2015 appropriations for the Department of Homeland Security, the Senate Appropriations Committee stated that:

"TSA should be commended for streamlining screening procedures for TSA Pre✓™ travelers, children under 12, senior citizens, flight attendants, and active duty military personnel. These expedited screening measures are beginning to yield security, budgetary, and economic benefits to both the agency and the flying public."¹⁴

Similarly, in its report on the proposed FY 2015 appropriations for DHS, the House Appropriations Committee stated that:

"The Committee is encouraged to see that TSA is actively pursuing efforts to better focus its resources and improve the passenger experience by applying risk-based security measures to its screening procedures."

"While TSA Pre✓™ offers great promise; a critical mass of participants is required for the program to achieve its objectives of enhanced security and efficiency. Therefore, the Committee directs TSA to continue to accelerate TSA Pre✓™ enrollment."¹⁵

TSA was well aware of the concerns about automating risk-based pre-screening [REDACTED] prior to implementing this policy decision. Viewing this matter in context with the numerous other improvements made to aviation security, current intelligence information, our counterterrorism mission, and other layers of security, the decision to automate designation for expedited screening or to [REDACTED] is a determination of the operational efficiencies gained or operational impact imposed. That decision falls within the category of establishing aviation security standards and regulations that is statutorily the responsibility of the TSA Administrator.¹⁶

[REDACTED] demonstrates our continuing assessment of potential low-risk populations. Assessing risk supports increasing the efficiency and effectiveness of [REDACTED] passenger screening system by allowing TSA to focus limited resources on those passengers about whom we know less, while providing expedited screening for those we know more about

¹⁴ U.S. Senate, Committee on Appropriations, Department of Homeland Security Appropriations Bill, 2015 Committee Report, S. Rept. 113-198, p. 71.

¹⁵ U.S. House, Committee on Appropriations, Department of Homeland Security Appropriations Bill, 2015 Committee Report, H. Rept. 113-481, p. 69.

¹⁶ See 49 U.S.C. § 114(d).

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed 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~~

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed 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.~~



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

SENSITIVE SECURITY INFORMATION

8

either as identified members of a trusted traveler population, or as members of groups for which there is little evidence of threats to transportation security.

TSA does not concur with restricting the use of [REDACTED]

ENCRYPTING COMMERCIAL AIRCRAFT CARRIER BOARDING PASSES [REDACTED]

TSA explored encrypting boarding pass barcodes and incorporating [REDACTED]. Following discussions with Airlines for America (A4A) and the International Air Transportation Association (IATA), TSA decided not to adopt this approach for two primary reasons. First, implementation is not feasible for some airline operators due to a limited number of available boarding pass fields in their systems. These fields are currently used to encode other information, and requiring airlines [REDACTED] would be disruptive to commercial business operations. Second, encrypting boarding pass barcodes is cost prohibitive. Airline stakeholders estimated the cost of compliance with a TSA security directive requiring barcode encryption was over \$500 million.¹⁷

Due to these considerations, TSA decided not to require encryption and adopted a more cost-effective digital signature approach to address the concerns associated with [REDACTED].

CREDENTIAL AUTHENTICATION TECHNOLOGY

Since 2009, TSA has pursued CAT, a system that would provide passenger prescreening information via a network connection to Secure Flight. The decision to leverage existing investments in Secure Flight and TSA's network infrastructure will significantly reduce industry cost and technical development while increasing the security of boarding pass data. TSA is moving forward with a phased implementation of CAT.

TSA's Office of Security Capabilities made a CAT award in April 2014. This award was for up to 12 systems that TSA will test against both functional and operational requirements to assess suitability and effectiveness. Testing is scheduled to begin in fall 2014 and, pending success,

¹⁷ INFORMATION MEMO from TSA Administrator John Pistole to DHS Secretary Janet Napolitano. *Printed Airline Boarding Pass Vulnerability*, October 25, 2012.

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed 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.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

SENSITIVE SECURITY INFORMATION

9

should be completed in early 2015. At that time, TSA expects to award full rate production and begin deploying CAT systems at all federalized airports.



WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed 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

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed 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.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

SENSITIVE SECURITY INFORMATION

U.S. Department of Homeland Security
Transportation Security Administration (TSA)

Response to **OIG Draft Letter Report, Alleged Use of the Risk-Based Rule** [REDACTED]
[REDACTED] Secure Flight [REDACTED]
[REDACTED] - Sensitive Security Information

Recommendation #1: Explore the feasibility of encrypting commercial aircraft carrier boarding passes [REDACTED].

TSA does not concur. Cost and feasibility were explored with stakeholders in 2012. TSA decided to pursue a more practical and affordable solution utilizing a digital signature.

Recommendation #2: Continue pursuing Credential Authentication Technology [REDACTED]
[REDACTED].

TSA Concur. TSA is pursuing Credential Authentication Technology and recently awarded a contract to begin operational test and evaluation of this technology. Based on this contract award, TSA believes the recommendation has been implemented and requests closure.

Recommendation #3: Ensure Credential Authentication Technology is fully functional [REDACTED]
[REDACTED].

TSA does not concur. The current level of risk associated with [REDACTED] is mitigated by a range of security procedures and technologies currently available and/or deployed by TSA.

Attachment

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed 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.

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed 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.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

SENSITIVE SECURITY INFORMATION

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



**Transportation
Security
Administration**

AUG - 8 2013

ACTION

MEMORANDUM FOR: John S. Pistole
Administrator, Transportation Security Administration

FROM: Victoria Newhouse /s/
Assistant Administrator, Office of Risk Based Security
Chair, Executive Risk Steering Committee

Kelly Hoggan /s/
Assistant Administrator, Office of Security Operations
Co-Chair, Executive Risk Steering Committee

THROUGH: John Halinski
Deputy Administrator

SUBJECT: TSA Pre✓™ Risk Assessment Rules,

ATTACHMENT: 1. TSA Pre✓™ Risk Assessment Rules
, RBS Principals Meeting, August 1, 2013
PowerPoint Presentation, Version 6 -

Purpose

The purpose of this memo is to obtain approval to
 TSA Pre✓™ expedited screening process.

Background

In January 2013, the RBS Executive Risk Steering Committee (ERSC) recommended implementing

WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this document 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.

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed 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

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

SENSITIVE SECURITY INFORMATION

2

As that concept moved forward to DHS for concurrence, Acting Deputy Secretary Beers raised concern about using [REDACTED] and asked for an independent evaluation of the [REDACTED] before moving forward with that component piece. As a result, the decision was made to [REDACTED] to allow TSA to move forward while external validation [REDACTED] was in process. On June 20, 2013, DHS Secretary Napolitano approved your request to implement TSA Pre✓™ Risk Assessment Rules [REDACTED] for TSA Pre✓™ expedited screening. This approach expands [REDACTED].

Adopting the expanded [REDACTED] is a reflection of our continuing assessments of potential low risk populations in support of our goal to expand the number of airports currently participating in TSA Pre✓™ and to achieve our goal of providing expedited screening to 25% of the traveling population by the end of calendar year 2013. This goal is further highlighted in the Senate Appropriations Committee FY2014 Report Language that requires you to certify no later than December 31, 2013, to the House and Senate Appropriation Committees that "...one in four air passengers that require security by the Transportation Security Administration is eligible for expedited screening without lowering security standards." Using [REDACTED] low risk passengers was independently validated by Mctron Inc., and provided to TSA and DHS in the *DHS S&T Rule Learning and Evaluation for TSA Secure Flight: Preliminary Results Report* published on October 5, 2012.

Discussion

It is important to remember that all passengers undergoing expedited screening are subject to physical security screening measures commensurate with or greater than international security standards. The TSA Pre✓™ Risk Assessment Rules do not use race, ethnicity, or national origin information. The approach taken to defining and implementing these risk assessment rules aligns with Secretary Napolitano's memorandum of April 26, 2013 regarding the nondiscriminatory use of race and ethnicity in screening and law enforcement activities.

Using [REDACTED] for calendar year 2012, and the No Fly List contained in the Terrorist Screening Data Base (TSDB from December 2012), a baseline level of relative risk for the entire passenger population was established. As noted in the *Meiron* report, statistical evaluation [REDACTED] indicates that [REDACTED] do correlate with risk with respect to acts of terrorism with an overall merit score¹ of [REDACTED] (merit in identifying both high and low risk passengers). Using [REDACTED] to classify passengers as low-risk has a merit score of [REDACTED], while the [REDACTED] have very low utility for classifying high-risk as reflected in a merit scores of just [REDACTED].

¹ Merit score reflects the accuracy of classification on a scale from 0.0 to 1.0, where 1.0 reflects perfect classification, 0.5 expected from random classification, and a value of 0.0 indicating misclassification of passengers by high or low risk.

WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this document 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.

SENSITIVE SECURITY 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 disclosed 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.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

Adding the [redacted] classification element of a Secure Flight rule set increases the merit score for low-risk travelers to [redacted].

The TSA ERSC established an integrated Project Team (IPT) consisting of representatives from Security Operations, Intelligence and Analysis, Security Capabilities and Risk Based Security offices to: 1) evaluate proposed [redacted] from a volume and systems risk perspective; 2) evaluate the relative risk of [redacted]; and, 3) provide recommendations to the ERSC regarding rules setting, risks, and potential mitigation actions. The IPT analysis shows several marked results useful in establishing [redacted] low risk traveler rules as follows:

[redacted]

During their analysis, the IPT identified three broad areas to consider [redacted] rules alone. Of primary concern to IPT members is that [redacted] are in development (e.g., Credential Authentication Technology, boarding pass scanners; airline boarding pass scanning verification solution; [redacted]) but none of these approaches are likely to be implemented by the end of Calendar Year 2013. Possible mitigation actions presented by the IPT in the near term included adopting [redacted]; increasing the amount of random and unpredictable screening performed in the TSA Pre✓ lane, frequently changing [redacted]. Each of these potential mitigation measures were associated with significant negative consequences or failed to address the specific issue of [redacted].

The two secondary areas of consideration raised by IPT members were potential impact on TSA credibility and the impact on TSA Pre✓™ Trusted Traveler program enrollment if the [redacted]

[redacted]

WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this document 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.

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed 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.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

SENSITIVE SECURITY INFORMATION

4

The ERSC considered several aspects of the proposed policy [REDACTED]
[REDACTED]
[REDACTED] international security standards. The ERSC also considered the negative aspects of each of the mitigation options identified by the IPT in light of the expected introduction of [REDACTED] within the next 6 months.

After discussing each of these matters, the ERSC decided to accept [REDACTED]
[REDACTED]
[REDACTED]

During ERSC deliberations, several general principles were agreed upon to guide this policy recommendation. First, the ERSC concurred that we should establish as the baseline level of acceptable risk [REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]

WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this document 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.

SENSITIVE SECURITY 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 disclosed 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

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

SENSITIVE SECURITY INFORMATION

5

The overall passenger risk profile [REDACTED] and the ERSC recommends

[REDACTED]

Under the proposal agreed to by the ERSC, [REDACTED]

[REDACTED]. The underlying assumption is that expedited screening for these low-risk passengers is provided at all domestic airport and entails expanding TSA Pre✓™ to the next 60 airports.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this document 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.

SENSITIVE SECURITY 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 disclosed 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.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

SENSITIVE SECURITY INFORMATION

6

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

The reverse logic of several of the above options is applicable as criteria for selecting where to apply [REDACTED]. Using the limited [REDACTED] capacity to further restrict application of [REDACTED] for flights [REDACTED] provides a practical application of intelligence information to inform the rules using similar risk logic that underscores FAMS flight scheduling and REFS activities. As example, [REDACTED]

WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this document 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.

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed 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.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

SENSITIVE SECURITY INFORMATION

7

[REDACTED]

In conjunction with existing TSA Pre✓™ eligibility, other expedited screening initiatives, and Managed Inclusion volume projections, the ERSC conservatively estimates that about 30% of the traveling public could receive expedited screening by the end of calendar year 2013 using the recommended baseline [REDACTED]

[REDACTED]

Next Steps:

Following approval of either recommendation 1 or 2 below, there remains a number of additional actions requiring completion prior to implementing TSA Pre✓™ Risk Assessment Rules

[REDACTED]

[REDACTED]

- Finalize outreach and communications plan to include:
 - House and Senate authorizing and appropriations committees.
 - TSA and DHS advisory committees
 - Privacy and Civil Liberties groups
 - Other government stakeholders (e.g., National Security Staff, Department of State, Department of Transportation)
 - TSA field leadership and workforce
 - Industry and trade associations
 - General public
- Approval of the TSA Pre✓™ Risk Assessment Rules review procedure by DHS.
- DHS Privacy Office to transmit the updated Secure Flight Systems of Record Notice (SORN) to incorporate TSA Pre✓™ Risk Assessment to the Office of Information and Regulatory Affairs (OIRA) within the Office of Management and Budget (OMB), and to Congressional oversight committees for 10 day review period, and the Privacy Impact Assessment (PIA) on the DHS website.
- Publication of the SORN in the Federal Register for a period of 30 days.

Recommendation 1:

Approve [REDACTED]
[REDACTED] The IPT and ERSC will
work to finalize specific low-risk [REDACTED]
[REDACTED]

WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this document 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.

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed 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.

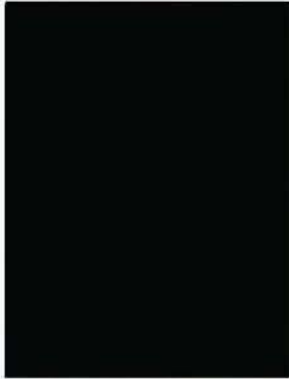


OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

SENSITIVE SECURITY INFORMATION

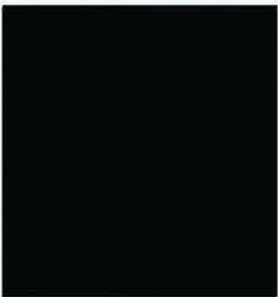
8



Approve *John S. Pistole* Disapprove _____
Modify _____ Needs More Discussion _____

Recommendation 2:

Approve _____
_____. The IPT and ERSC will work to finalize specific _____
_____. As part of that effort, the ERSC will review and validate the current update to the
Current Airport Threat Assessment (CATA) document.



Approve _____ Disapprove _____
Modify _____ Needs More Discussion _____

WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this document 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.

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed 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.

ADDITIONAL INFORMATION

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General (OIG) Office of Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov, or follow us on Twitter at: [@dhsoig](https://twitter.com/dhsoig).

OIG HOTLINE

To expedite the reporting of alleged fraud, waste, abuse or mismanagement, or any other kinds of criminal or noncriminal misconduct relative to Department of Homeland Security (DHS) programs and operations, please visit our website at www.oig.dhs.gov and click on the red tab titled "Hotline" to report. You will be directed to complete and submit an automated DHS OIG Investigative Referral Submission Form. Submission through our website ensures that your complaint will be promptly received and reviewed by DHS OIG.

Should you be unable to access our website, you may submit your complaint in writing to:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Office of Investigations Hotline
245 Murray Drive, SW
Washington, DC 20528-0305

You may also call 1(800) 323-8603 or fax the complaint directly to us at (202) 254-4297.

The OIG seeks to protect the identity of each writer and caller.