

~~SENSITIVE SECURITY INFORMATION~~

U.S. Department of Homeland Security
Transportation Security Administration
6595 Springfield Center Drive
Springfield, VA 20598-6002



Transportation
Security
Administration

Mr. [REDACTED]
Special Counsel
Office of Special Counsel

RE: OSC File No. DI-20-000038 (Addendum)

Dear Mr. [REDACTED]:

The attached report is in response to the January 28, 2020 referral of the above-captioned matter to the Secretary of the Department of Homeland Security (DHS) regarding a disclosure received by your office. This referral served as an amendment of OSC's initial referral on November 14, 2019. The Secretary referred this inquiry to the Transportation Security Administration (TSA) for investigation and response. Consistent with delegations from the DHS Secretary and Undersecretary for Management, I am the designated official authorized to oversee the investigation and take any appropriate action determined to be necessary in accordance with 5 U.S.C. §1213(d). The Department's findings are included in the attached Report of Investigation.

OSC characterized Federal Security Director (FSD) [REDACTED] disclosure as follows: (1) a policy allowing Supervisory Transportation Security Officers to make a judgment call on whether a passenger with no documentation should proceed through security is based solely on an arbitrary wait time (over 30 minutes) to receive a response from the Identity Verification Call Center (IVCC); (2) permitting Federal Security Directors (FSDs) to reduce the use of lights and loupes [REDACTED] creates an unnecessary security gap; and (3) providing passengers who present a personally printed PreCheck™ boarding pass, which cannot be scanned by a Boarding Pass Scanner (BPS), an option to proceed through security using standard security lanes creates security vulnerabilities.

The procedures that the whistleblower outlines in his disclosure relate to the Travel Document Checker (TDC) position. The Transportation Security Officer acting in the TDC position is responsible for verifying a passenger's identity and confirming that he or she has a valid boarding pass. The procedures a TDC officer must follow are largely delineated in the Checkpoint & Specialized Screening (CSS) Standard Operating Procedures (SOP) and Operations Directive (OD) 400-50-1-35: Travel Document Checker – Alternative Protocol and Requirements, both distributed to the workforce at the end of 2019. The procedures in the documents are not new, rather they were a result of a consolidation project, which combined

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~~

procedures from four SOPs into one. The OD provides two specific alternatives to the travel document verification requirements of the CSS SOP.

In regard to disclosure (1), an IVCC wait time exceeding 30 minutes is a rare occurrence, having only occurred on 20 days over the past 10 years. Should this nonetheless occur, the OD provides that a TSA representative will assess the passenger for suspicious behavior, and determine whether to refer the passenger for Selectee screening or deny entry into the screening checkpoint. This procedure does not add a significant security vulnerability because an adversary would not know when the IVCC is significantly delayed and, even if an individual was allowed to be screened given this process, Selectee screening is the highest level of screening conducted by TSA.

Regarding disclosure (2), lights and loupes technology is a tool used by a TDC officer to check for possibly fraudulent identification. Its use may be reduced from [REDACTED] to [REDACTED] during peak travel periods for no more than 30 minutes at a time. The likelihood of an individual exploiting this procedure is remote, given the limited time that this screening protocol may be implemented. Further, there are additional procedures in place to mitigate any increased risk, such as the physical inspection of the identification, observed behavior, validation by the IVCC (if needed), and the discretion to refer an individual to Selectee screening.

Disclosure (3) involves passengers whose self-printed TSA PreCheck™ boarding pass cannot be properly scanned by the BPS. The CSS SOP allows a passenger the option of obtaining another boarding pass or entering standard screening after a TSA representative conducts name matching determines the passenger's screening status (PreCheck™, Standard, or Selectee). This process does not present a significant vulnerability as an individual would need to match a boarding pass with an appropriate identification and correct flight information. If suspicious behavior is observed by the TDC officer, that passenger will be pulled for additional screening.

The Agency is currently deploying technology that will significantly change the TDC process, as it relates to disclosures (2) and (3). TSA began deploying Credential Authentication Technology (CAT) units in 2019 and, where operational, is now the primary tool used by TDC officers to authenticate and verify the validity of an individual's identification and confirm that individual's existing flight reservation. Presently, over 1,000 CAT units have been deployed to airports, with an estimated completion date of 2026. The use of CAT units will significantly reduce the use of lights and loupes to verify the authenticity of an identification, and lights and loupes will only be used if the CAT unit is inoperable or cannot read a specific piece of identification. CAT units also reduce a TDC officer's need to visually inspect a boarding pass (including those that are personally printed), and a BPS will only be used as a secondary method when a CAT unit is not available or with minors who may not possess an acceptable form of identification.

Please note that this report contains Sensitive Security Information (SSI) that is controlled under 49 C.F.R. Parts 15 and 1520 must be handled and protected accordingly, and cannot be publicly released. TSA's SSI office will conduct a review and redaction of the report for public release which will be forwarded to you as soon as possible. Per the request of OSC, the Agency will also redact all employee names included in the report.

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~~

If you require further information regarding these matters, please do not hesitate to contact [REDACTED] in the Chief Counsel's office at [REDACTED].

Sincerely yours,

[REDACTED]
Digitally signed by [REDACTED]

Date: 2021.03.23 10:58:18
-04'00'

Acting Deputy Administrator

cc:

[REDACTED]
Assistant Administrator
Domestic Aviation Operations
Security Operations

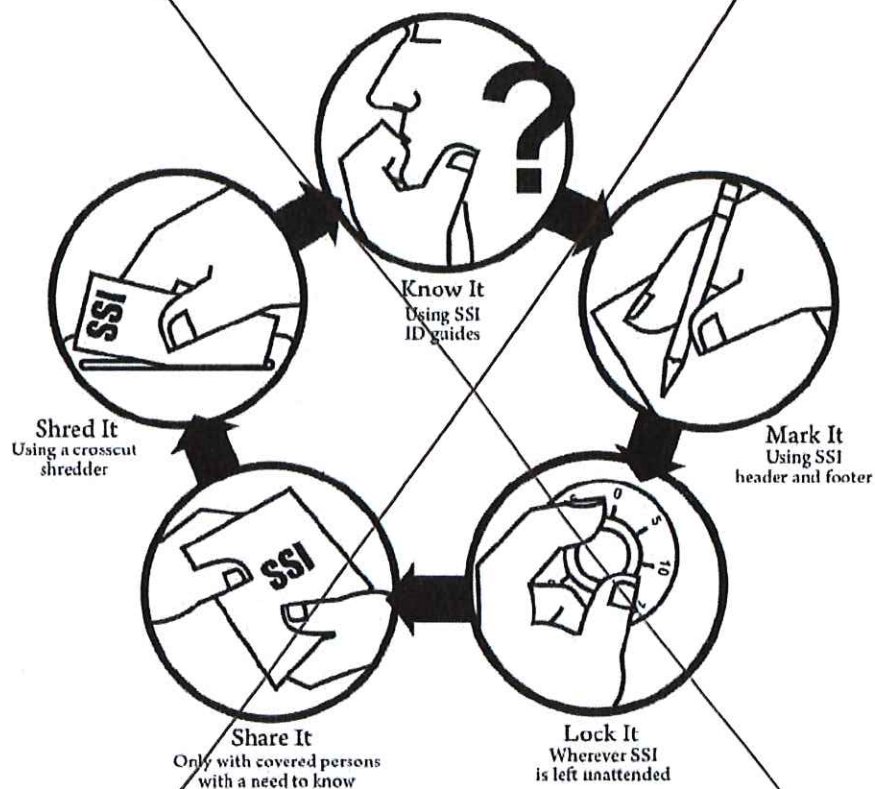
[REDACTED]
Assistant Administrator
Requirements and Capabilities Analysis

~~**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.~~

DEPARTMENT OF HOMELAND SECURITY

SENSITIVE SECURITY INFORMATION

Cover Sheet



For more information on handling SSI, contact SSI@dhs.gov.

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~~



U.S. DEPARTMENT OF HOMELAND SECURITY TRANSPORTATION SECURITY ADMINISTRATION TSA INVESTIGATIONS

REPORT OF INVESTIGATION

CASE NUMBER: I20 0358

PR CASE: No

TITLE: OSC Case Referral for Investigation (Addendum) DI-20-000038

CROSS REFERENCED CASES: I19 0386-Office of Special Counsel Disclosure
(DI-20-000038)

SUBJECT:

Name: Transportation Security Administration

Duty title: N/A

Pay band: N/A

Duty location: N/A

EOD: N/A

Administrative Status: N/A

ALLEGATION(S): 5 U.S.C. 1213(c) – TSA officials implemented three (3) new screening procedures and protocols that present a substantial likelihood of gross mismanagement and a specific danger to public safety.

PERIOD OF INVESTIGATION: November 27, 2020 – March 15, 2021

CASE STATUS: Closed

INVESTIGATED BY: Special Agent [REDACTED] and Transportation Security Specialist [REDACTED]

REPORT BY: Special Agent [REDACTED]

March 18, 2021

Date

[REDACTED]
Special Agent in Charge
Washington Field Office
TSA Investigations

WARNING: THIS RECORD CONTAINS SENSITIVE SECURITY INFORMATION THAT IS CONTROLLED UNDER 49 CFR PART 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~~

Report of Investigation
I20 0358

Page 2

REPORT DISTRIBUTION

- ☐ Director, Professional Responsibility
- ☒ Chief Counsel
- ☐ Executive Assistant Administrator/Director, Federal Air Marshal Service
- ☐ Executive Assistant Administrator, Security Operations
- ☐ Executive Assistant Administrator, Operations Support
- ☐ Executive Assistant Administrator, Enterprise Support
- ☒ Other – Office of Special Counsel
- ☒ File

Report of Investigation (ROI) Handling: The ROI and information contained herein are subject to the Privacy Act of 1974 (5 U.S.C. 552A, Public Law 93-579) and thus may not be released outside official channels. This material must be safeguarded from unauthorized disclosure, and should not be left unattended or discussed with unauthorized persons, and must be retained in a security container when not in use.

This report is provided to management to take appropriate action. Outside of the official adjudicative process this report or any portion thereof may not be released to the subject of the investigation or any individual identified therein, or their representatives, or reproduced without the written consent of TSA Investigations.

WARNING: THIS RECORD CONTAINS SENSITIVE SECURITY INFORMATION THAT IS CONTROLLED UNDER 49 CFR PART 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~~

Report of Investigation
I20 0358

Page 3

SUMMARY OF FINDINGS FOR OFFICE OF SPECIAL COUNSEL:

The Office of Special Counsel's referral for investigation stipulated that the report of investigation include:

1) *A summary of Information with respect to which the investigation was initiated;*

On November 25, 2020, Transportation Security Administration (TSA) Investigations (INV) was notified by TSA Chief Counsel of a whistleblower disclosure addendum to a previous disclosure case (OSC File No. DI-20-000038) bringing forward three (3) additional allegations regarding the issuance of TSA, Security Operations (SO), Operations Directive (OD) 400-50-1-35: Travel Document Checker – Alternative Protocol and Requirements, dated December 12, 2019 and the Checkpoint & Specialized Screening (CSS) Standard Operating Procedures (SOP), dated November 13, 2019. The disclosure was made by Federal Security Director (FSD) [REDACTED].

Specifically, the whistleblower alleged that:

- I. A policy allowing a Supervisory Transportation Security Officer (STSO) to make a judgement call on whether a passenger with no documentation should proceed through security is based solely on an arbitrary wait time (greater than 30 minutes) in receiving a response from the Identity Verification Call Center (IVCC).
- II. Permitting a FSD to reduce the use of ultraviolet lights and loupes from [REDACTED] creates an unnecessary security gap.
- III. Providing passengers who present a personally printed PreCheck™ boarding pass an option to proceed through security using standard security lanes creates security vulnerabilities. **(Exhibits 1, 2 & 3)**

2) *A description of the conduct of investigation;*

The whistleblower was interviewed and requested to provide verbal and written documentation explaining his disclosure. TSA officials from SO, Requirements and Capabilities Analysis (RCA), Inspection (INS), and Acquisitions (ACQ) were interviewed and asked to provide verbal and written documentation. The individuals interviewed are listed in the table below under the heading "Other Persons Associated with the Case". Audio recordings of interviews will be maintained in the case file.

WARNING: THIS RECORD CONTAINS SENSITIVE SECURITY INFORMATION THAT IS CONTROLLED UNDER 49 CFR PART 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~~

Report of Investigation
I20 0358

Page 4

Multiple documents were reviewed and analyzed including the OD and CSS SOP; Chapter 2, Section 2B, mentioned by the whistleblower. These documents are included in Exhibits 2 & 3, archived SOPs in Exhibits 5 & 6, as well as call data from the Identity Verification Call Center (IVCC) for a ten-year period included in Exhibit 7.

3) *A summary of any evidence obtained from the investigation;*

Background

The Travel Document Checker (TDC) function is vital to the TSA layered approach in ensuring security for civil aviation. The TDC officer is generally the first Transportation Security Officer (TSO) a passenger will interact with. TDC officers are located at a podium, and individuals are unable to pass the TDC area and continue to the screening checkpoint without having their identification and travel documents checked. An individual provides the TDC with his/her travel documents and identification, and the TDC directs the passenger to the screening lane consistent with the vetting status. An individual may be denied entry into the sterile area as a result of TDC screening procedures.

The main responsibilities of the TDC officer is to verify an individual's identity; confirm travel documents (that the individual has a valid boarding pass for travel within the acceptable timeframe) and; confirm and direct the individual to the appropriate level of screening: PreCheck™, Standard, or Selectee. The TDC process is accomplished prior to any individual continuing through the screening checkpoint.¹

Several tools and procedures are available to the TDC to ensure that they are successful in carrying out this important function.

The Boarding Pass Scanner (BPS) is used by the TDC officer to validate the various types of travel documents. These include paper travel documents that are self-printed, Kiosk-generated, or Aircraft operator printed, and mobile boarding passes stored on electronic media devices. With the use of the BPS, the TDC officer is also able to validate the correct screening status (PreCheck™, Standard, or Selectee) as visually marked on the boarding pass. Following BPS verification, the TDC officer will proceed with name matching

¹ Checkpoint & Specialized Screening (CSS) Standard Operating Procedures (SOP), dated November 13, 2019, Part A: Travel Document Check; Chapter 1 General Policies,

WARNING: THIS RECORD CONTAINS SENSITIVE SECURITY INFORMATION THAT IS CONTROLLED UNDER 49 CFR PART 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~~

Report of Investigation
I20 0358

Page 5

procedures whereby the name on the Identification document (ID) is matched to the information included on the boarding pass.²

Further, the TDC officer is required to validate the authenticity of ID that are presented to them. To assist the TDC officer in determining the authenticity of ID, ultraviolet (black) lights and magnifying loupes are provided to check for the presence of security features that are usually included on all IDs. The use of lights and loupes also allows the TDC officer to observe signs of tampering [REDACTED]

[REDACTED]³

When individuals are not able to present any acceptable or valid ID, TSA has procedures in place to attempt to verify their identity. In these cases, the IVCC, which is part of TSA Intelligence and Analysis (I&A)/National Transportation Vetting Center (NTVC), is contacted and attempts will be made to verify the identity of the individual.⁴

During a DHS-OIG audit of TSA in 2012, vulnerabilities were found in determining fraudulent ID and boarding passes. As a result of this audit, TSA began work on requirements to mitigate these identified vulnerabilities. Credential Authentication Technology (CAT), was the result of this research and development.

TSA began deploying CAT units to airports in 2019 and, where operational, is now the primary tool used by TDC officers to authenticate and verify an individual's identity, flight information, and screening status. This is accomplished by scanning an individuals' passport or driver's license (or other types of card ID), into the CAT unit. The CAT unit scans for biographical information from the ID such as full name, Date of Birth, and gender, and this information is automatically forwarded to Secure Flight and matched with flight reservation data.

A deployed CAT unit provides the TDC officer both the validity of ID presented as well as confirmation of matching that ID to an existing flight reservation. This provides the officer with the necessary information to determine that the individual has a need to be present at the

² CSS SOP, Part A: Travel Document Check; Chapter 2 - ID and Travel Document Verification Procedures; Section 2 - Verifying Travel Document.

³ CSS SOP, Part A: Travel Document Check; Chapter 2 - ID and Travel Document Verification Procedures; Section 1 - Verifying Identity Document.

⁴ CSS SOP, Part A: Travel Document Check; Chapter 2 - ID and Travel Document Verification Procedures; Section 4 - Individuals Without Acceptable ID.

WARNING: THIS RECORD CONTAINS SENSITIVE SECURITY INFORMATION THAT IS CONTROLLED UNDER 49 CFR PART 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~~

Report of Investigation
I20 0358

Page 6

screening checkpoint. Additionally, the CAT unit will provide the individual's screening status (PreCheck™, Standard, or Selectee), allowing for the TDC officer to direct the individual to the proper screening lane.

To date, a total of 1,053 CAT units have been deployed to airports, with an additional 467 units planned for deployment by the end of Calendar Year (CY) 2021. An additional 601 CAT units are expected to be deployed by the end of CY 2022. It is anticipated that a total of 2,121 CAT units will be operational at airports by the end of CY 2022. Additionally, a new full operational capability number of 3,585 units has been established that will achieve the goal of having CAT units at all security checkpoints. Based on new technical requirements and funding, it is expected that TSA will achieve this goal by the end of CY 2026. **(Exhibit 4)**

A review of an SO/FSD Communication memorandum, dated November 13, 2018⁵ from the AA of Domestic Aviation Operations, showed that the new CSS SOP was developed to improve the manner in which screening information was conveyed to the workforce and consolidated four (4) already existing SOPs into one document. The CSS SOP did not contain any new policies or procedures. The CSS SOP was created to assist the field with locating procedural information more quickly. Additionally, on December 12, 2019, Operations Directive (OD) 400-50-1-35: Travel Document Checker – Alternative Protocol and Requirements – was published. This OD allowed FSDs to use alternatives to identification verification requirements outlined in the CSS SOP, specifically regarding the use of lights and loupes during peak travel periods and when the IVCC response wait time exceeded 30 minutes. Use of these alternatives is discretionary on the part of the FSD.

On November 13, 2019, the new CSS SOP was released reflecting an implementation date of no later than December 31, 2019. Under Chapter 2-Verifying Travel Document; Section B - Validate Travel Document with Boarding Pass Scanner (BPS); Table A.1, a screening protocol is listed advising screening personnel how to handle a TSA PreCheck™ passenger whose self-printed boarding pass cannot be scanned by the Boarding Pass Scanner (BPS). Specifically, the SOP provides two options for the passenger: "go to the aircraft operator or kiosk to obtain a paper travel document; or receive standard screening after conducting Name Matching and Determine Individual's Screening Status." **(Refer to Exhibit 2)**

⁵ This document appears misdated and should read "November 13, 2019."

WARNING: THIS RECORD CONTAINS SENSITIVE SECURITY INFORMATION THAT IS CONTROLLED UNDER 49 CFR PART 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~~

Report of Investigation
I20 0358

Page 7

OD-400-50-1-35 outlines two (2) specific alternative screening protocols that may be used at the discretion of FSDs in the Travel Document Checker (TDC) process. These procedures may only be implemented during peak travel periods, and are discretionary on the part of the FSD.

One of the protocols listed in the OD consist of procedures involving the reduction in the use of ultraviolet lights and magnifying loupes to verify ID from [REDACTED] during peak travel periods. Specifically, the OD provides FSDs or their designees the option to: reduce the use of black lights and loupes from [REDACTED] when verifying identification documents provided by passengers processing through the security checkpoint. This alternative protocol [REDACTED]
[REDACTED]

The second protocol involves procedures when wait times for the IVCC to assist in verifying the identity of individuals who are not in possession of acceptable ID exceeds thirty minutes. The OD permits FSDs or designees to authorize STSOs to use the following alternative process:

If a STSO, in consultation with a Behavior Detection (BD) certified TSO, determines that an individual does not exhibit suspicious behavior, a Transportation Security Manager (TSM) may refer the individual to selectee screening. A TSA representative will determine whether the individual will be allowed to proceed into the sterile area based on the individual's conduct during the selectee screening process, and the results of selectee screening. If an individual exhibits suspicious behaviors, the TSM must deny the individual entry into the screening checkpoint and sterile area and, if appropriate, notify law enforcement.⁶ **(Refer to Exhibit 3)**

The whistleblower alleges that the protocols outlined in the CSS SOP and OD 400-50-1-35 create security gaps or vulnerabilities and were only implemented to enhance customer service and reduce wait times in the screening lanes.

- I. A policy allowing a Supervisory Transportation Security Officer (STSO) to make a judgement call on whether a passenger with no documentation should proceed

⁶ Operations Directive (OD)-400-50-35: Travel Document Checker – Alternative Protocol and Requirements

~~SENSITIVE SECURITY INFORMATION~~

Report of Investigation
I20 0358

Page 8

through security is based solely on an arbitrary wait time (in excess of 30 minutes) in receiving a response from the Identity Verification Call Center (IVCC).

One of the primary functions of the IVCC is to assist airport TSA representatives in attempting to verify the identity of individuals who have no acceptable forms of identification (ID) on their person during the screening process. This specific process allows passengers to still continue with their travel as well as satisfying any security issues that may arise as a result of an individual not having acceptable ID.

OD 400-50-1-35 permits FSDs or their designees the discretion to implement certain protocols in response to experiencing IVCC wait times in excess of 30 minutes to verify an individual's identity. The OD specifies that if a STSO in consultation with a BD trained TSO determines that an individual does not exhibit suspicious behaviors, a TSM may refer the individual to Selectee screening. Based on the conduct of the individual during the Selectee screening process and the results, a TSA representative will determine if the individual will be allowed to proceed. If the individual does exhibit suspicious behavior, they must be denied entry into the screening checkpoint and a Law Enforcement Officer (LEO) may be notified. Therefore, in this situation, the individual will either receive Selectee screening, the highest level of screening TSA provides, or be denied entry into the screening checkpoint.

The RCA/Procedures Branch Manager (BM) and SO/Standards & Directives Division Management Analyst (MA) stated that this specific screening protocol was not new and has been part of policy for many years. As part of the 2019 SOP consolidation project by SO and RCA, the screening protocol was pulled from the now cancelled Travel Document Checker (TDC) SOP Revision 2, Change 4, Chapter 4, Section 7 and published in OD 400-50-1-35. The language from the SOP remained essentially unchanged when included in OD 400-50-1-35. **(Exhibits 5 & 6)**

Call data for the IVCC was obtained from the NTVC Operations Analysis BM to determine the frequency that wait times over 30 minutes occurred. A review of the data indicated that for the period from November 1, 2010 to January 21, 2021, only 20 days within this period was discovered to have an occasion where the maximum wait time for assistance from the IVCC exceeded thirty (30) minutes. This data confirms the comments by both the whistleblower and the RCA/Procedures BM that this is a rare occurrence. **(Exhibit 7)**

~~WARNING: THIS RECORD CONTAINS SENSITIVE SECURITY INFORMATION THAT IS CONTROLLED UNDER 49 CFR PART 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~~

Report of Investigation
I20 0358

Page 9

An Inspection/Unconventional Threats/BM involved in covert testing of screening and security procedures was interviewed, and it was his opinion that the protocol outlined in this OD was the best approach for TSA since the individual will ultimately be directed to Selectee screening procedures, which is the highest level of screening that TSA conducts. **(Exhibit 8)**

The SO/Assistant Administrator (AA) of Domestic Aviation Operations provided that she does not believe this was an arbitrary time that was established as alleged by the whistleblower. She was of the opinion that time measurements and other evaluations were probably conducted to determine an acceptable amount of time for the IVCC to respond to a request from the field. Additionally, in response to this complaint, she said that STSOs are empowered to make security decisions at the security checkpoint and evaluate information that they have before them. If an ID is not produced, based on their training and experience, TSA allows them to make decisions on how to proceed. This protocol allows many factors to be evaluated to ensure that a level of security is accomplished and passengers are able to proceed. Also, given the infrequency that wait times exceeding 30 minutes occurs, she does not feel that there is a need to either revise or remove this protocol since the passenger will be afforded Selectee screening, the highest level offered by TSA. **(Exhibit 9)**

The RCA/AA was interviewed and stated that it was his opinion that allowing an individual to pass through the screening checkpoint without the proper ID when the identity of the individual could not be verified because the wait time for a response from the IVCC exceeded 30 minutes does not add a significant security vulnerability. This opinion was based on the randomness of the situation. He believes that an adversary intending to do harm could not possibly know to show up at a checkpoint at the exact time, knowing that the IVCC is significantly delayed in assisting with identity verification, and expect to be allowed to proceed through the screening process. Additionally, when allowed, the individual is subjected to the highest level of screening conducted by TSA, -Selectee screening. He also believes that this is the best approach for TSA in handling individuals who come to the security checkpoint and do not have the required ID. **(Exhibit 10)**

- II. Permitting a Federal Security Director (FSD) to reduce the use of lights and loupes from [REDACTED] creates an unnecessary security gap

WARNING: THIS RECORD CONTAINS SENSITIVE SECURITY INFORMATION THAT IS CONTROLLED UNDER 49 CFR PART 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~~

Report of Investigation
I20 0358

Page 10

Ultraviolet or black lights and magnifying loupes is a tool used by a TDC officer to check for the presence of security features on all IDs presented to them as well as visually observing if the ID may have been fraudulently printed. This allows the TDC officer to determine if an ID is authentic or possibly fraudulent requiring additional scrutiny and involvement of law enforcement.

The RCA/Procedures/BM provided information that the reduction in the use of ultraviolet lights and magnifying loupes during peak travel periods has been in existence for many years. Supporting documentation provided to INV by the BM reflected that this specific screening protocol dates as far back as 2008 and was included in Aviation Security/Screening Management SOP, dated May 12, 2008. The section of the SOP in 2008 that spoke to the reduction of its use during peak travel periods was Section 2A-3, Alternative Travel Document Checking Procedures. This specific section authorized FSDs at their discretion to reduce the use to as low as 25% during peak travel periods. This was later revised, date unknown, to only allow a [REDACTED] **(Refer to Exhibit 5)**

As reported above, according to the SO/MA, this alternative screening protocol was included in TDC SOP Revision 2, Change 4, Chapter 4, Section 7. The information was subsequently pulled from this SOP and included in SO/OD 400-50-1-35: Travel Document Checker – Alternative Protocol and Requirements – dated December 12, 2019, under Requirements, Section A. The OD provides specific alternatives to ID verification requirements of the CSS SOP, which was developed as a result of the SOP consolidation project. Section A of the OD allows FSDs or their designees the discretion to reduce the use of ultraviolet lights and magnifying loupes during peak travel periods [REDACTED] When implemented, [REDACTED]

[REDACTED] **(Refer to Exhibit 6)**

The RCA/Identity Management Capability/BM and INS/Unconventional Threats/BM advised that with the deployment to the airports of the new CAT units, the actual use of ultraviolet lights and magnifying loupes to verify the authenticity of ID by the TDC officer will be significantly reduced. The CAT units, where deployed and operational, will become the primary tool to determine the authenticity of ID by reading the numerous and different security features present in an acceptable ID document. The use of ultraviolet lights and magnifying loupes will remain as an alternative when the CAT unit is either inoperable or cannot read a specific ID. **(Exhibit 11 & refer to Exhibit 8)**

WARNING: THIS RECORD CONTAINS SENSITIVE SECURITY INFORMATION THAT IS CONTROLLED UNDER 49 CFR PART 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~~

Report of Investigation
I20 0358

Page 11

The SO/AA provided information that the use of ultraviolet lights and magnifying loupes is an effective security tool used by TDC officers to recognize if an ID may have been tampered with or is possibly fraudulent. Further, she explained that there are now other technologies available that can enhance TSA's ability to detect tampered IDs and mentioned the deployment of the new CAT units. She acknowledged that the use of the CAT units will reduce the need to use lights and loupes as a TDC function.

According to the SO/AA, there were past concerns with the ultraviolet lights and loupes equipment used and this was one of the many reasons why the CAT units were developed. She did advise though that the use of ultraviolet lights and loupes will remain as an alternative to the CAT units, as the CAT units are not presently deployed at all airports, and occasionally the unit may be inoperable. Further, it was her opinion that the limited reduction in the use of lights and loupes is not a security vulnerability. ID is still being physically checked, name matching procedures to the boarding pass is taking place, and the individual is still being screened. She also provided an example that, during peak travel periods, reducing the ultraviolet lights and loupes technology may ensure that large crowds of unscreened individuals do not gather in front of the screening checkpoint, which, in her opinion, could create a security vulnerability.

The SO/AA disagreed with the whistleblower's assertion that a FSD would be criticized if one of the protocols listed was not implemented in response to wait times at the security checkpoint. She explained that an FSD should never feel compelled to implement a protocol that he/she was not comfortable with. **(Refer to Exhibit 9)**

The Acquisitions (ACQ)/Program Manager (PM) responsible for managing the CAT program was interviewed and explained that the deployment of CAT units will diminish the use of ultraviolet lights and magnifying loupes. Where operational, the CAT unit is intended to be the primary tool used by a TDC officer to authenticate an individual's identity by matching the biographical data from an ID to a flight reservation for the day, and confirm the individual's screening status. The ACQ/PM provided that the CAT SOP states that CAT is now to be used as the primary tool for identity verification, and ultraviolet lights and loupes technology will only be used when the CAT unit is inoperable or cannot scan an ID. **(Refer to Exhibit 4)**

The RCA/AA was interviewed and provided his opinion that the alternative screening protocol of reducing the use of ultraviolet lights and loupes does not create any additional security vulnerability. His opinion is based on the fact that CAT units have been deployed at many

~~**WARNING:** THIS RECORD CONTAINS SENSITIVE SECURITY INFORMATION THAT IS CONTROLLED UNDER 49 CFR PART 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~~

Report of Investigation
I20 0358

Page 12

airports, and in the present environment, with passenger volume decreased, he believes that most passengers are encountering CAT during the screening process.

The RCA/AA also is of the opinion that, based on the unpredictability of this reduction as reflected in the OD, the likelihood of someone intentionally exploiting this procedure is remote, given the limited time that this alternative screening protocol may be implemented. He opined that, with other procedures in place such as the physical inspection of the ID, observed behavior characteristics of the individual, identity validation by the IVCC if needed, and the discretion at the checkpoint to refer an individual to Selectee screening, relieves this protocol from being a major vulnerability.

Additionally, the RCA/AA explained a new device called the Enhanced Document Imager (EDI), which was developed as a better solution to use rather than the magnifying loupes to help identify fraudulent or tampered ID. TSA began deploying these new devices to airports in June 2020. The EDI is a high powered magnifying glass with an associated light that will magnify a credential to such a degree to allow the TDC officer to more easily discern the micro printing on a specific ID. He further stated that when a CAT unit is not able to read a ID, the EDI will take the place of magnifying loupes, because it will enable the TDC officer to better observe many of the security features imbedded into the credential. The RCA/AA also related that with the use of CAT and the EDI as an alternative, the need to use magnifying loupes will be alleviated. He did say though that the use of the lights and loupes technology will still need to be used until the EDI is fully deployed. The AA could not provide an estimated timeframe for full deployment of the EDI technology. **(Refer to Exhibit 10)**

- III. Providing passengers who present a personally printed PreCheck™ boarding pass that cannot be properly scanned by the BPS the option to proceed through security using standard security lanes creates security vulnerabilities

Boarding Pass Scanners (BPS) are used by TDC officers to validate travel documents that are presented to them during the screening process. These documents may come in the following formats: self-printed, Kiosk generated, aircraft operator representative-printed, or mobile that are stored on smartphone or tablets. The BPS validates certain information such as name of the passenger, flight information, and screening status i.e.: PreCheck™, Selectee, or Standard. The BPS allows the TDC officer to name match the boarding pass to

WARNING: THIS RECORD CONTAINS SENSITIVE SECURITY INFORMATION THAT IS CONTROLLED UNDER 49 CFR PART 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

Report of Investigation
I20 0358

Page 13

the ID presented and to ensure that a passenger receives the appropriate level of screening. In the Checkpoint & Specialized Screening SOP, dated November 13, 2019, Table A.1, (shown below) allows for an individual with a self-printed TSA PreCheck™ boarding pass that cannot be verified the option of obtaining another boarding pass from the aircraft operator or enter standard screening after a TSA representative has conducted name matching procedures and determined the appropriate screening status:

Table A.1: BPS Verification and Resolution ⁷	
Self-printed TSA Pre✓® boarding passes	Green Light: Proceed to NAME MATCHING and DETERMINE INDIVIDUAL'S SCREENING STATUS.
	Yellow or Red Light: Direct the individual options to go to the aircraft operator or kiosk to obtain a paper travel document; or receive standard screening after conducting NAME MATCHING and DETERMINE INDIVIDUAL'S SCREENING STATUS.

The RCA/Procedures/BM provided information that the CSS SOP procedure outlined above was not new and was also taken from an existing SOP as part the SOP consolidation project. A review of the now cancelled TDC SOP, Revision, 2, Change 4 document reflects that the same procedure was contained in the cancelled SOP. The procedure is now included in the new CSS SOP, dated November 13, 2019. (Refer to Exhibit 6, Attachment B)

The RCA/ Identity Management Capability /BM and INS/Unconventional Threats/BM provided information that, as reported with the lights and loupes reduction protocol, the new CAT units presently being deployed will be used to provide all of the necessary information to the TDC officer in assessing not only the authenticity of the ID presented but also the information contained in a boarding pass. Once the CAT unit validates the authenticity of an ID, the biographical information from the ID is sent to Secure Flight where the information is matched to flight reservation information and screening status. As a result, the TDC officer

⁷ CSS SOP, Part A: Travel Document Check; Chapter 2 – ID and Travel Document Verification Procedures; Section 4 – Verifying Travel Document; Paragraph B. Travel Document with the Boarding Pass Scanner (BPS).

WARNING: THIS RECORD CONTAINS SENSITIVE SECURITY INFORMATION THAT IS CONTROLLED UNDER 49 CFR PART 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~~

Report of Investigation
I20 0358

Page 14

will now not be required to review the paper or mobile boarding passes, as all of the information will be automated. **(Refer to Exhibits 8 & 11)**

Without the consideration of CAT, the RCA/ Identity Management Capability /BM did not agree with the whistleblower's example that someone can simply pick up a discarded boarding pass and attempt to present it as authentic to gain entry to the sterile area. In his opinion, additional procedures by the TDC such as matching the name on the boarding pass to a valid identification document will alert the TDC that the boarding pass is not authentic. **(Refer to Exhibit 11)**

The INS/Unconventional Threats/BM provided additional information that his team has conducted covert testing in the past regarding the use of the BPS by the TDC officer. The testing consisted of both [REDACTED]. He was not able to provide the results of the testing since it is at a classified level. He did relate that with the deployment of the CAT machines, the allegations raised by the whistleblower will be negated. **(Refer to Exhibit 8)**

The SO/AA does not believe that the examples given by the whistleblower regarding TSA PreCheck™ boarding passes is likely to occur given the additional security layers that are in place. She said an individual attempting to accomplish this would have to align many factors to include matching up the boarding pass with an appropriate ID, correct flight information, etc. If any anomaly is observed by the TDC officer, that individual will be pulled for additional screening. **(Refer to Exhibit 9)**

The ACQ/PM when interviewed stated that with the deployment of CAT units, the use of BPS to authenticate information on the travel boarding passes will be reduced, since the TDC officer will no longer need to visually inspect the boarding pass for the required information. He explained that once the ID is validated, the biographical information is automatically sent to Secure Flight where it is determined if the individual has a flight reservation for the day at that specific airport, as well as the appropriate screening status. According to the ACQ/PM, this process is a more reliable and efficient method in validating this information. As for this specific protocol, where a TSA PreCheck™ passenger whose self-printed boarding pass cannot be scanned is afforded the option to enter standard screening or return to the aircraft operator for another boarding pass, he believes with the deployment of CAT there would be no reason to implement this protocol.

~~**WARNING:** THIS RECORD CONTAINS SENSITIVE SECURITY INFORMATION THAT IS CONTROLLED UNDER 49 CFR PART 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~~

Report of Investigation
I20 0358

Page 15

The ACQ/PM related that when an individual's flight information cannot be verified by the CAT unit, the CAT unit will return a result of "Check BP." If the information on the boarding pass cannot be verified, the individual is referred back to the aircraft operator to obtain a new boarding pass. At no time during this process, is an individual provided the option to enter screening until all ID verification and name matching procedures are successfully resolved. As with light and loupes, the ACQ/PM also stated that the BPS will be the secondary method used when CAT is not available or with minors who may not possess an ID. **(Refer to Exhibit 4)**

The RCA/AA was interviewed and stated that, in his opinion, allowing a TSA PreCheck™ passenger whose self-printed boarding pass could not be scanned by the BPS the option to enter standard screening or return to the airline operator for a new boarding pass does not create a security vulnerability. As he explained, other security layers or mitigation efforts are in place that significantly reduce the possibility that the system can be exploited. Given the example that the whistleblower provided in the OSC disclosure, that a high risk individual can simply retrieve a discarded self-printed boarding pass and present it as their own at the screening checkpoint and proceed through security, the RCA/AA responded that this possibility is very remote. He further explained that this was unlikely to occur because the individual would have to exactly match the information from the boarding pass to an ID. With the use of EDI, ultraviolet lights and loupes, and name matching procedures, having a fraudulent boarding pass will not do the adversary any good without a very good fraudulent ID and there are very solid measures in place, in his opinion, to defeat this potential vulnerability. Additionally, once all ID procedures are completed to include identity verification through the IVCC, if needed, if there is any question as to the identity or motivation of the individual, he/she will be referred to selectee screening procedures.

As further related by the RCA/AA, with CAT now being deployed, the need for an individual to present a physical boarding pass to include one that is self-printed is negated. He explained that the CAT units will now assess the validity of an ID by reading the various imbedded security features. Once the ID is determined to be valid, the information from the ID is linked to Secure Flight to determine if the individual has a flight reservation for that date at that specific airport as well as the appropriate screening status. Adding all of these tools together in an automated system is an enormous enhancement to security effectiveness, throughput, and convenience for the passenger. According to the RCA/AA, the goal of TSA is

WARNING: THIS RECORD CONTAINS SENSITIVE SECURITY INFORMATION THAT IS CONTROLLED UNDER 49 CFR PART 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

Report of Investigation
I20 0358

Page 16

to deploy CAT units to all airports and said that the number of units needed to reach full deployment is still being determined. **(Refer to Exhibit 10)**

4) *A listing of any violation or apparent violation of any law, rule, or regulation;*

INV found no violation or apparent violation of any law, rule, or regulation.

5) *A description of any action taken or planned as a result of the investigation;*

Though no known action is planned to be taken as a result of this investigation, TSA has been developing technology that will fully automate the TDC function at the screening checkpoints. As previously mentioned, TSA is currently deploying CAT units to the airports with the intent of having them fully deployed at all airports by the end of CY 2026 (dependent on funding). Implementing this technology will negate the need for passengers to present a paper boarding pass to the TDC and all necessary required information, for example name matching to a travel reservation and screening status, will become fully automated. Additionally, the CAT units will be used to authenticate any required and accepted ID that is presented by passengers. This method will diminish the practice of the TDC officer having to visually check the authenticity of ID by using ultraviolet lights and magnifying loupes or EDI, except in those rare occasions that an ID cannot be read by the CAT unit or the machine is inoperable.

As for the effect on calls to the IVCC for assistance to verify the identity of individuals who come to the screening checkpoint without acceptable ID, CAT does not address this issue. It is anticipated that the current screening procedures in place will continue in attempting to verify the identity of individuals. When a TSA representative experiences a wait time for assistance from the IVCC exceeding 30 minutes, the alternative screening protocol providing FSDs or their designees the discretion to refer an individual to Selectee screening will continue.

WARNING: THIS RECORD CONTAINS SENSITIVE SECURITY INFORMATION THAT IS CONTROLLED UNDER 49 CFR PART 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~~

Report of Investigation
I20 0358

Page 17

OTHER INVESTIGATIVE ASPECTS

Persons Associated with the Case:

Name	Role	Title	Office	Exhibit
[REDACTED]	Whistleblower	Federal Security Director (FSD)	SO	12
[REDACTED]	Witness	Assistant Administrator (AA)	RCA	10
[REDACTED]	Witness	Management Analyst (MA)	SO	6
[REDACTED]	Witness	Branch Manager (BM)/CAT Program	ACQ	4
[REDACTED]	Witness	Branch Manager (BM)/ Identity Management Capability	RCA	11
[REDACTED]	Witness	BM/Procedures	RCA	5
[REDACTED]	Witness	AA/Domestic Aviation Operations	SO	9
[REDACTED]	Witness	BM/Unconventional Threats	INS	8

WARNING: THIS RECORD CONTAINS SENSITIVE SECURITY INFORMATION THAT IS CONTROLLED UNDER 49 CFR PART 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~~

Report of Investigation
I20 0358

Page 18

EXHIBITS	
1	Memorandum of Activity (MOA) – Review of U.S. Office of Special Counsel memo, dated January 28, 2020 and TSA Chief Counsel memo, dated November 25, 2020.
2	MOA – Review of SO, Checkpoint & Specialized Screening; Standard Operating Procedures (SOP), dated November 13, 2019.
3	MOA - Review of Security Operations (SO), Operations Directive (OD)-400-50-1-35: Travel Document Checker – Alternative Protocol and Requirements.
4	MOI of ACQ/PM [REDACTED] and attached written statement, dated March 10, 2021.
5	MOI of RCA/BM [REDACTED] and attached written statement, dated February 16, 2021 and Screening Management SOP, Section 2A-3. Alternative Travel Document Checking Procedures, dated May 12, 2008; Pages 6-7.
6	MOI of SO/MA [REDACTED] and attached written statement, dated February 2, 2021 and cancelled TDC SOP, Revision 2, Change 4, dated September 30, 2019; pages: 2-4, 2-5, 4-7 and 4-8.
7	MOA – Review of IVCC Call data provided by I&A/NTVC/BM [REDACTED].
8	MOI of INS/BM [REDACTED] and attached written statement, dated February 16, 2021.
9	MOI of SO/AA [REDACTED] and attached written statement, dated March 1, 2021.
10	MOI of RCA/AA [REDACTED] and attached written statement, dated March 10, 2021.
11	MOI of RCA/BM [REDACTED] and attached written statement, dated March 15, 2021.
12	Memorandum of Interview (MOI) of FSD [REDACTED] and attached written statement, dated December 23, 2020.

WARNING: THIS RECORD CONTAINS SENSITIVE SECURITY INFORMATION THAT IS CONTROLLED UNDER 49 CFR PART 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.

Exhibit 1

SENSITIVE SECURITY INFORMATION



TSA INVESTIGATIONS MEMORANDUM OF INTERVIEW OR ACTIVITY

Type of Activity: <input type="checkbox"/> Personal Interview <input type="checkbox"/> Telephone Interview <input checked="" type="checkbox"/> Records Review <input type="checkbox"/> Other	Date and Time: November 30, 2020 9:30 am
Activity or Interview of: Review of Office of Special Counsel (OSC) memo, dated January 28, 2020 and TSA Chief Counsel (CC) memo, dated November 25, 2020	Conducted by: Special Agent [REDACTED] Transportation Security Specialist [REDACTED] Location of Interview/Activity: Residence (Due to COVID-19)

Subject Matter/Remarks

A review of OSC memo, dated January 28, 2020 and TSA CC memo, dated November 25, 2020 was conducted on November 30, 2020. The following information was obtained from that review:

- A Whistleblower Disclosure, Addendum to OSC File No. DI-20-000038 was forwarded on January 28, 2020 to the Department of Homeland Security (DHS) requesting that three additional allegations made by Federal Security Director (FSD) [REDACTED] be reviewed and investigated. **(Attachment A)**
- On November 25, 2020, TSA CC forwarded a memo to TSA Investigations (INV) stating that the DHS Office of General Counsel had informed TSA that the DHS-Office of Inspector General had declined investigation of this OSC disclosure addendum and that INV was now required to conduct an investigation. **(Attachment B)**
- TSA FSD [REDACTED] disclosed that TSA officials updated airport security procedures that he alleges may constitute gross mismanagement and a substantial and specific danger to public safety. The three additional allegations made by FSD [REDACTED] in the addendum were as follows:

Case Number I20 0358	Case Title: OSC Case Referral for Investigation (Addendum) DI-20-000038
-------------------------	--

WARNING: This record contains SENSITIVE SECURITY INFORMATION that is controlled under 49 CFR PART 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, Washington, DC 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~~

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

1. A TSA Security Operations, Operations Directive, effective December 12, 2020, now permits FSDs to authorize Supervisory Transportation Security Officers to make a judgement call on whether or not to allow a passenger who produces no documentation to proceed through security based solely on an arbitrary wait time in receiving a response from the Identity Verification Call Center and;
2. Permits an FSD to reduce the use of lights and loupes from [REDACTED] creating an unnecessary security gap by permitting individuals with questionable identification to proceed through security without verification.
3. TSA Checkpoint & Specialized Screening Standard Operating Procedures, Chapter 2, Tables A.1 and A.2, effective November 13, 2019, now provides passengers who present a personally printed PreCheck™ boarding pass, which cannot be scanned at security checkpoints, an option to proceed through security using standard security lanes creating security vulnerabilities.

Attachments:

- A. Office of Special Counsel memo, dated January 28, 2020
- B. TSA Chief Counsel memo, dated November 25, 2020

Case Number: I20 0358	Case Title: OSC Case Referral for Investigation (Addendum) DI-20-000038
--------------------------	--

Revised May 1, 2018

WARNING: This record contains ~~SENSITIVE SECURITY INFORMATION~~ that is controlled under 49 CFR PART 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, Washington, DC 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.

Attachment A



U.S. OFFICE OF SPECIAL COUNSEL
1730 M Street, N.W., Suite 300
Washington, D.C. 20036-4505

The Special Counsel

January 28, 2020

The Honorable [REDACTED]
Acting Secretary
Department of Homeland Security
245 Murray Lane, S.W.
Washington, D.C. 20528

Re: OSC File No. DI-20-000038
Referral for Investigation--5 U.S.C. § 1213(c)

Dear Acting Secretary [REDACTED]:

This letter serves to amend OSC's initial referral sent on November 14, 2019. At that time, I referred to you a whistleblower disclosure alleging that officials at the Department of Homeland Security, Transportation Security Administration (TSA), Washington, D.C., engaged in actions that constitute gross mismanagement and a substantial and specific danger to public safety.¹ Following this referral for investigation, the whistleblower, Federal Security Director [REDACTED] who consented to the release of his name, disclosed additional allegations related to TSA's updated airport security procedures.² I write again to alert you to their seriousness. Specifically, Mr. [REDACTED] alleged:

- (1) Pursuant to OD-400-50-1-35 TSA, para. B, TSA now permits FSDs to authorize Supervisory Transportation Security Officers (STSOs) to allow passengers who do not have identification to proceed through security when Identity Verification Call Center (IVCC) response times are greater than 30 minutes. IVCC staff run background checks on passengers without identification to determine their identity. Mr. [REDACTED] alleged that the new policy allows STSOs to make a judgement call on whether a passenger with no documentation should proceed through security based solely on the arbitrary wait time to receive a response from IVCC.

¹See OSC File No. DI-20-000038.

²The Department of Homeland Security has designated the information discussed in this referral as Sensitive Security Information. Pursuant to the agency's September 28, 2018, email request, OSC has marked this letter accordingly.

The Honorable [REDACTED]
January 28, 2020
Page 2 of 3

- (2) Pursuant to TSA Operations Directive OD-400-50-1-35, para. A (December 12, 2019), TSA now permits Federal Security Directors (FSDs) to reduce the use of lights and loupes [REDACTED] of passengers passing through screening. Black lights and loupes are used to more closely examine questionable travel documents that lack obvious security features. Lights and loupes are used most frequently at larger, international airports where many different types of identification are encountered. Mr. [REDACTED] alleged that this creates an unnecessary security gap by permitting individuals with questionable identification to proceed through security without verification.
- (3) Pursuant to TSA Checkpoint & Specialized Screening Standard Operating Procedures, Ch. 2, Tables A.1 and A.2 (November 13, 2019) passengers who present a personally printed Pre-Check boarding pass, which cannot be scanned by TSA boarding pass scanners at security checkpoints, may be given the option to proceed through security using standard security lanes. The new process is used in lieu of requiring such individuals to obtain an official boarding pass from their airline. Mr. [REDACTED] explained that this could permit an individual with no legitimate boarding pass—for example, a passenger who picked up a discarded boarding pass or printed a faked boarding pass—to proceed through security and into the airport secure area without a legitimate purpose. Mr. [REDACTED] further noted that all individual passenger screening levels, including elevated risk status, are encoded within the boarding pass bar code. Thus, there is now the possibility that individuals on TSA's No-Fly List, who are prohibited from entering the sterile area of any airport, and individuals designated as "selectees" who require additional screening, could access the sterile area of an airport after only undergoing standard screening procedures.

Pursuant to my authority under 5 U.S.C. § 1213(c), I have concluded that there is a substantial likelihood that the allegations provided to OSC disclose gross mismanagement and a substantial and specific danger to public safety. I am requesting that you incorporate these new allegations into your pending investigation in OSC File No. DI-20-000038 and provide one report to OSC that addresses all the allegations.³

Please note that specific allegations and references to specific violations of law, rule, or regulation are not intended to be exclusive. If, in the course of your investigation, you discover additional violations, please include your findings on these additional matters in the report to OSC. As previously noted, your agency must conduct an investigation of these matters and produce a report, which must be reviewed and signed by you. Per statutory requirements, I will review the report for sufficiency and

³I have attached my November 14, 2019 referral letter in this matter for your reference.

SENSITIVE SECURITY INFORMATION

The Honorable [REDACTED]

January 28, 2020

Page 3 of 3

reasonableness before sending copies of the agency report, along with the whistleblower's comments and any comments or recommendations I may have, to the President and congressional oversight committees and making these documents publicly available.

Additional important requirements and guidance on the agency report are included in the attached Appendix, which can also be accessed at <https://osc.gov/Services/Pages/DU-Resources.aspx#tabGroup01>. If your investigators have questions regarding the statutory process or the report required under 5 U.S.C. §1213, please contact [REDACTED] Chief, Disclosure Unit, at [REDACTED] for assistance. I am also available for any questions you may have.

Sincerely,



Special Counsel

Enclosures

cc: The Honorable [REDACTED] Inspector General

APPENDIX
AGENCY REPORTS UNDER 5 U.S.C. § 1213

GUIDANCE ON 1213 REPORT

- OSC requires that your investigators interview the whistleblower at the beginning of the agency investigation when the whistleblower consents to the disclosure of his or her name.
- Should the agency head delegate the authority to review and sign the report, the delegation must be specifically stated and include the authority to take the actions necessary under 5 U.S.C. § 1213(d)(5).
- OSC will consider extension requests in 60-day increments when an agency evidences that it is conducting a good faith investigation that will require more time to complete.
- Identify agency employees by position title in the report and attach a key identifying the employees by both name and position. The key identifying employees will be used by OSC in its review and evaluation of the report. OSC will place the report without the employee identification key in its public file.
- Do not include in the report personally identifiable information, such as social security numbers, home addresses and telephone numbers, personal e-mails, dates and places of birth, and personal financial information.
- Include information about actual or projected financial savings as a result of the investigation as well as any policy changes related to the financial savings.
- Reports previously provided to OSC may be reviewed through OSC's public file, which is available here: <https://osc.gov/Pages/Resources-PublicFiles.aspx>. Please refer to our file number in any correspondence on this matter.

RETALIATION AGAINST WHISTLEBLOWERS

In some cases, whistleblowers who have made disclosures to OSC that are referred for investigation pursuant to 5 U.S.C. § 1213 also allege retaliation for whistleblowing once the agency is on notice of their allegations. The Special Counsel strongly recommends the agency take all appropriate measures to protect individuals from retaliation and other prohibited personnel practices.

EXCEPTIONS TO PUBLIC FILE REQUIREMENT

OSC will place a copy of the agency report in its public file unless it is classified or prohibited from release by law or by Executive Order requiring that information be kept secret in the interest of national defense or the conduct of foreign affairs. 5 U.S.C. § 1219(a).

EVIDENCE OF CRIMINAL CONDUCT

If the agency discovers evidence of a criminal violation during the course of its investigation and refers the evidence to the Attorney General, the agency must notify the Office of Personnel Management and the Office of Management and Budget. 5 U.S.C. § 1213(f). In such cases, the agency must still submit its report to OSC, but OSC must not share the report with the whistleblower or make it publicly available. See 5 U.S.C. §§ 1213(f), 1219(a)(1).



U.S. OFFICE OF SPECIAL COUNSEL
1730 M Street, N.W., Suite 300
Washington, D.C. 20036-4505

The Special Counsel

November 14, 2019

The Honorable [REDACTED]
Acting Secretary
Department of Homeland Security
245 Murray Lane, S.W.
Washington, D.C. 20528

Re: OSC File No. DI-20-000038
Referral for Investigation--5 U.S.C. § 1213(c)

Dear Acting Secretary [REDACTED]

I am referring to you for investigation a whistleblower disclosure that officials at the Department of Homeland Security, Transportation Security Administration (TSA), Washington, D.C., engaged in actions that constitute gross mismanagement and a substantial and specific danger to public safety. A report of your investigation of these allegations and any related matters is due to the Office of Special Counsel on January 13, 2020.

[REDACTED] a Federal Security Director, who consented to the release of his name, disclosed that TSA officials have approved airport security policies that place public safety at risk.¹ Specifically, the allegation to be investigated is that:

- TSA officials implemented procedures for combining standard and Pre-Check security lanes that introduce exploitable security gaps into the passenger screening process.

[REDACTED] disclosed that in April 2019 TSA officials mandated a new security process called "blended lanes" at airports nationwide.² Blended lanes permit TSA officials to combine Pre-Check, standard passenger, and crew member screening in one security lane at airports that do not maintain a dedicated Pre-Check lane, or during times when maintaining a dedicated Pre-Check lane is not feasible.

[REDACTED] alleged that the screening procedures for blended lanes include multiple steps that increase opportunities for human error and introduce exploitable gaps in the security

¹The Department of Homeland Security has designated the standard operating procedures discussed in this referral as Sensitive Security Information. Pursuant to the agency's September 28, 2018, email request, OSC has marked this letter accordingly.

²TSA Security Operations, Leader Rollout Guidance: Blended Lane TSA Pre ✓ Operations (April 21, 2019)

SENSITIVE SECURITY INFORMATION

The Honorable [REDACTED]
November 14, 2019
Page 2 of 3

screening process. For example, in a blended lane, the TSA Travel Document Checker is required to identify Pre-Check passengers and provide them with a Pre-Check card to present to the Divestiture Officer. Mr. [REDACTED] argues that there are no controls in place to prevent an individual from passing his or her Pre-Check or crew card to a standard passenger, immediately introducing a potential security gap into the process.³

Mr. [REDACTED] alleged that the screening process used in "blended lanes" is confusing and unwieldy and that there are inadequate measures in place to control the vetting indicators after screening is completed. According to Mr. [REDACTED], after identifying the status of the passenger, agency guidance requires the Divestiture Officer to place a colored brick known as a "vetting indicator" in front of each passenger's property on the screening belt, letting the X-ray operator know which level of screening the property should receive—crew, Pre-Check, standard, or comprehensive screening for passengers designated as high-risk. The X-ray operator must also flip a manual Pre-Check/standard switch at the X-ray machine each time the screening level changes to assist in keeping track of the appropriate screening level for each item. After screening, the Property Search Officers are required to collect the vetting indicators and return them to the Divestiture Officer for reuse. Mr. [REDACTED] further alleged that requiring employees to screen Pre-Check and standard passengers at random intervals via the same X-ray machine increases the likelihood that errors will occur.

Mr. [REDACTED] noted that TSA introduced the use of blended lanes [REDACTED]

[REDACTED] Mr. [REDACTED] further noted that, to his knowledge, there has been no analysis of the potential security concerns inherent in the screening process for blended lanes in light of TSA's continued failure to meet basic screening proficiency. Thus, Mr. [REDACTED] alleged that the introduction of blended lanes compromises TSA's ability to screen passengers properly and places the public at risk of exploitable security gaps in the screening process.

Pursuant to my authority under 5 U.S.C. § 1213(c), I have concluded that there is a substantial likelihood that the information provided to OSC discloses gross mismanagement and a substantial and specific danger to public safety. Please note that specific allegations and references to specific violations of law, rule, or regulation are not intended to be exclusive. If, in the course of your investigation, you discover additional violations, please include your findings on these additional matters in the report to OSC. As previously noted, your agency must conduct

³Also of concern, and as noted in our referral dated July 26, 2018, is that the majority of Pre-Check passengers are selected from the general passenger population based on a computer algorithm that assesses their security risk. The whistleblower argues that they have not received prior enhanced security scrutiny and that the introduction of blended lanes further reduces the level of screening these passengers receive.

The Special Counsel

~~SENSITIVE~~ SECURITY INFORMATION

The Honorable [REDACTED]
November 14, 2019
Page 3 of 3

an investigation of these matters and produce a report, which must be reviewed and signed by you. Per statutory requirements, I will review the report for sufficiency and reasonableness before sending copies of the agency report, along with the whistleblower's comments and any comments or recommendations I may have, to the President and congressional oversight committees and making these documents publicly available.

Additional important requirements and guidance on the agency report are included in the attached Appendix, which can also be accessed at <https://osc.gov/Pages/DOW.aspx>. If your investigators have questions regarding the statutory process or the report required under 5 U.S.C. §1213, please contact [REDACTED], Chief, Disclosure Unit, at [REDACTED] for assistance. I am also available for any questions you may have.

Sincerely,



[REDACTED]
Special Counsel

Enclosure

cc: The Honorable [REDACTED], Inspector General

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.

Attachment B

~~SENSITIVE SECURITY INFORMATION~~

U.S. Department of Homeland Security

Office of Chief Counsel
601 South 12th Street
Arlington, VA 20598



**Transportation
Security
Administration**

MEMORANDUM

To: [REDACTED]
Director of Investigations
TSA Investigations (INV)

From: [REDACTED] [REDACTED]
Principal Deputy Chief Counsel (Acting)
Chief Counsel

Date: November 25, 2020

Subject: Whistleblower Disclosure, Addendum to OSC File No. DI-20-000038

Chief Counsel's office has become aware of a whistleblower disclosure filed with the U.S. Office of Special Counsel (OSC), which alleges that TSA officials implemented procedures that may constitute gross mismanagement and a substantial and specific danger to public safety. The specific allegations made by whistleblower [REDACTED], a Federal Security Director, are described in the attached letter from OSC to Acting Secretary [REDACTED]. According to OSC, the allegations to be investigated are: (1) a policy allowing Supervisory Transportation Security Officers to make a judgment call on whether a passenger with no documentation should proceed through security is based solely on an arbitrary wait time to receive a response from the Identity Verification Call Center; (2) permitting Federal Security Directors to reduce the use of lights and loupes from [REDACTED] creates an unnecessary security gap; and (3) providing passengers who present a personally printed PreCheckTM boarding pass an option to proceed through security using standard security lanes creates security vulnerabilities.

Pursuant to 5 U.S.C. § 1213, the Special Counsel has determined that there is a substantial likelihood that the information provided discloses gross mismanagement, and a substantial and specific danger to public safety. Consequently, the agency is required to conduct an investigation of the allegations and prepare a report for the Special Counsel. 5 U.S.C. § 1213(c).

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~~

On November 25, 2020 the DHS Office of General Counsel (OGC) has informed us that the DHS Office of Inspector General has declined the opportunity to investigate this matter. Therefore, TSA Investigations is required to conduct an investigation.

OSC requires that the investigation include an interview of the whistleblower. In addition, the report of investigation must include:

- (1) a summary of the information with respect to which the investigation was initiated;
- (2) a description of the conduct of the investigation;
- (3) a summary of any evidence obtained from the investigation;
- (4) a listing of any violation or apparent violation of any law, rule or regulation; and
- (5) a description of an action taken or planned as a result of the investigation, such as:
 - a. changes in agency rules, regulations or practices;
 - b. the restoration of any aggrieved employee;
 - c. disciplinary action against any employee; and
 - d. referral to the Attorney General of any evidence of criminal violation.

Pursuant to 5 U.S.C. § 1213(e), OSC must transmit a copy of the report to the complainant, unless it contains evidence of a criminal violation, which has been referred to the Attorney General. I note that ultimately OSC will provide the report, among other things, to the President and the congressional committees with jurisdiction over DHS/TSA.

If you have any questions concerning this matter, please contact [REDACTED], an attorney in my office, who may be reached at [REDACTED]. Please also keep her apprised of the status of this investigation so that she may inform the DHS OGC and OSC of developments.

cc: [REDACTED]
Deputy Administrator

Exhibit 2

SENSITIVE SECURITY INFORMATION



TSA INVESTIGATIONS MEMORANDUM OF INTERVIEW OR ACTIVITY

Type of Activity: <input type="checkbox"/> Personal Interview <input type="checkbox"/> Telephone Interview <input checked="" type="checkbox"/> Records Review <input type="checkbox"/> Other	Date and Time: December 4, 2020 11:00am
Activity or Interview of: Review of Security Operations (SO), Checkpoint & Specialized Screening (CSS); Standard Operating Procedures (SOP), dated November 13, 2019	Conducted by: Special Agent [REDACTED] Transportation Security Specialist [REDACTED] TSA Investigations Location of Interview/Activity: Residence (Due to COVID-19)

Subject Matter/Remarks

On December 4, 2020, a review of SO, Checkpoint & Specialized Screening (CSS) SOP, dated November 13, 2019 was conducted. This SOP, specifically Chapter 2, Tables A.1 and A.2, is the subject of one of the allegations by Federal Security Director (FSD) [REDACTED] in his Whistleblower disclosure addendum. The following information was obtained from that review:

- As noted in the OSC addendum from [REDACTED], Chapter 2, Table A.1 BPS Verification and Resolution of the SOP, dated November 13, 2019 does state that a passenger who presents a self-printed TSA PreCheck™ boarding pass that cannot be scanned and/or verified using the Boarding Pass Scanner (BPS) has the option to proceed by utilizing the standard screening lanes or obtain a paper travel document from the airline operator or kiosk. Specifically, this table is located in Part A: Travel Document Check, Chapter 2; Section 2. Verifying Travel Document; Paragraph B. Validate Travel Document with the Boarding Pass Scanner (BPS)
- Table A.2 of the same section was also mentioned in [REDACTED] OSC disclosure addendum. A review of information contained in this table, however, shows that it does not specifically refer to only PreCheck™ passengers, but BPS Notifications and Resolution for all passengers whose boarding pass could not be validated or the format not recognized. According to the table, a BPS notification of an incorrectly formatted boarding pass may indicate that it is

Case Number I20 0358	Case Title: OSC Case Referral for Investigation (Addendum) DI-20-000038
-------------------------	--

WARNING: This record contains SENSITIVE SECURITY INFORMATION that is controlled under 49 CFR PART 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, Washington, DC 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~~

MEMORANDUM OF INTERVIEW OR ACTIVITY (continuation sheet)

fraudulent. All passengers who present a boarding pass that fits into one of these categories reflected in Table A.2 are sent back to the aircraft operator for a new boarding pass. There is no mention of any passenger, to include PreCheck™ passengers, being provided the option to receive standard screening.

- In CSS SOP, Chapter 2, Section 4(B) (12), there is a reference to the procedures to be taken when the wait time for assistance from the Identity Verification Call Center (IVCC) exceeds 30 minutes. It states that a TSA representative must notify an STSO who will then notify the FSD/ FSD designee to request permission to use alternative identity verification and screening procedures. This section of the SOP appears to be in direct reference to OD-400-35-1 that was communicated to the FSDs on December 12, 20019 as explained in Exhibit 2 of this report.
(Attachment B)
- With the release of this CSS SOP, four (4) SOPs and a quick reference guide were cancelled. Also, no additional policies and procedures are contained in the new CSS SOP.
(Attachment C)

A copy of CSS SOP, dated November 13, 2019 will be maintained in the case file.

Attachments:

- A. CSS SOP, Chapter 2: ID and Travel Document Verification, Section 2(B): Validate Travel Document with Boarding Pass Scanner (BPS), Table A.1 and A.2, pages; 18-20.
- B. CSS SOP, Chapter 2: ID and Travel Document Verification, Section 4(B) (12): Establish Identity Through IVCC, pages; 23-25. Travel Document.
- C. SO, FSD Communication, 400.5 – ROUTINE – Release of Checkpoint & Specialized Screening SOP, dated November 13, 2018.

Case Number: I20 0358	Case Title: OSC Case Referral for Investigation (Addendum) DI-20-000038
--------------------------	--

Revised May 1, 2018

WARNING: This record contains SENSITIVE SECURITY INFORMATION that is controlled under 49 CFR PART 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, Washington, DC 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.

Attachment A

~~SENSITIVE SECURITY INFORMATION~~

[Go Back](#)

Version 1

Release Date: November 13, 2019

Implementation Date: Determined Locally (No Later Than December 31, 2019)

— Chapter 2: ID and Travel Document Verification Procedures —

Checkpoint & Specialized Screening SOP

~~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 PENALTIES OR OTHER ACTION. FOR U.S. GOVERNMENT AGENCIES, PUBLIC DISCLOSURE GOVERNED BY 5 U.S.C. 552 AND 49 CFR PARTS 15 AND 1520.

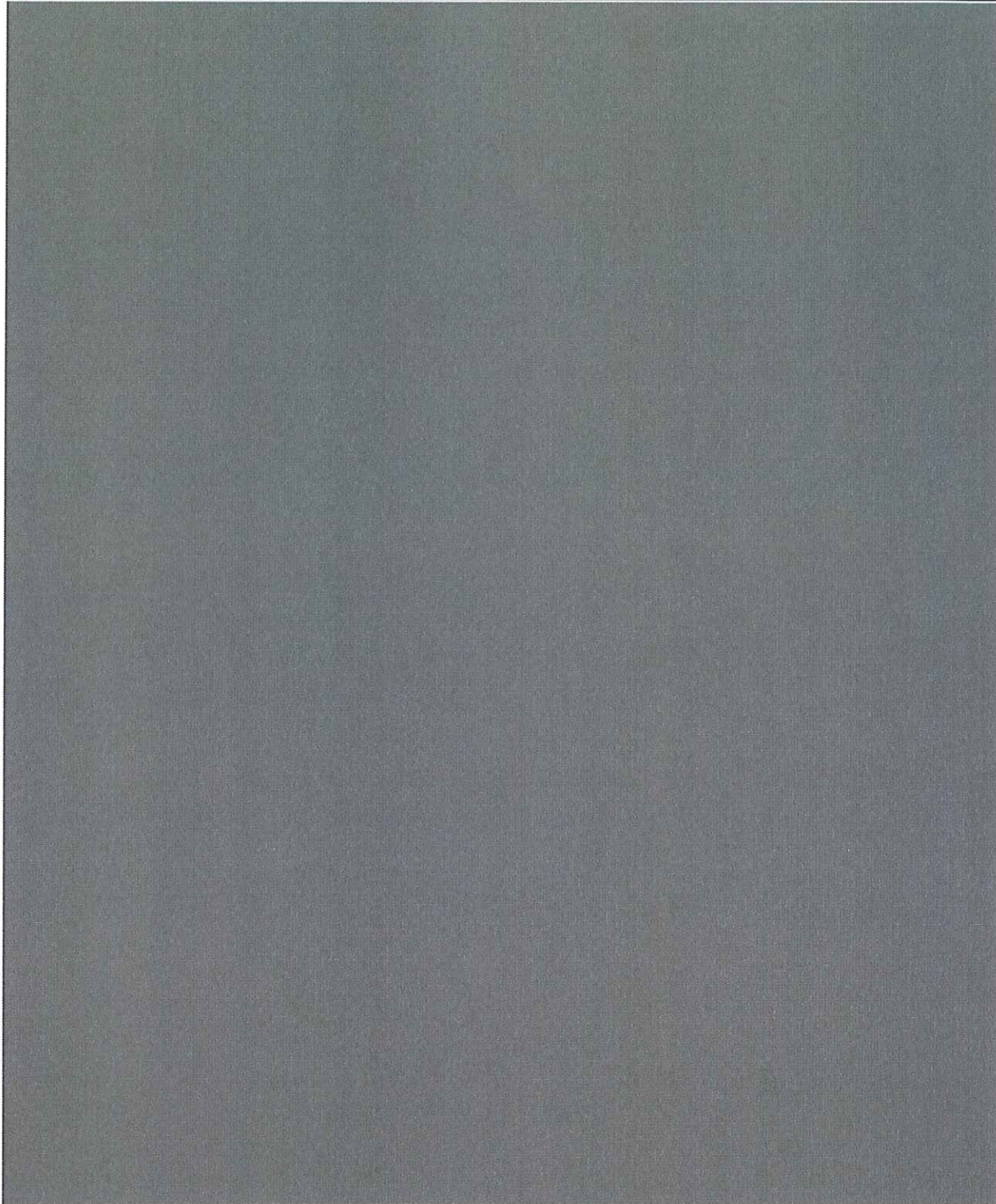
~~SENSITIVE SECURITY INFORMATION~~

[Go Back](#)

Version 1

Release Date: November 13, 2019

Implementation Date: Determined Locally (No Later Than December 31, 2019)



— Chapter 2: ID and Travel Document Verification Procedures —

Checkpoint & Specialized Screening SOP

~~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 PENALTIES OR OTHER ACTION. FOR U.S. GOVERNMENT AGENCIES, PUBLIC DISCLOSURE GOVERNED BY 5 U.S.C. 552 AND 49 CFR PARTS 15 AND 1520.

~~SENSITIVE SECURITY INFORMATION~~

[Go Back](#)

Version 1

Release Date: November 13, 2019

Implementation Date: Determined Locally (No Later Than December 31, 2019)

— Chapter 2: ID and Travel Document Verification Procedures —

Checkpoint & Specialized Screening SOP

~~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 PENALTIES OR OTHER ACTION. FOR U.S. GOVERNMENT AGENCIES, PUBLIC DISCLOSURE GOVERNED BY 5 U.S.C. 552 AND 49 CFR PARTS 15 AND 1520.

Attachment B

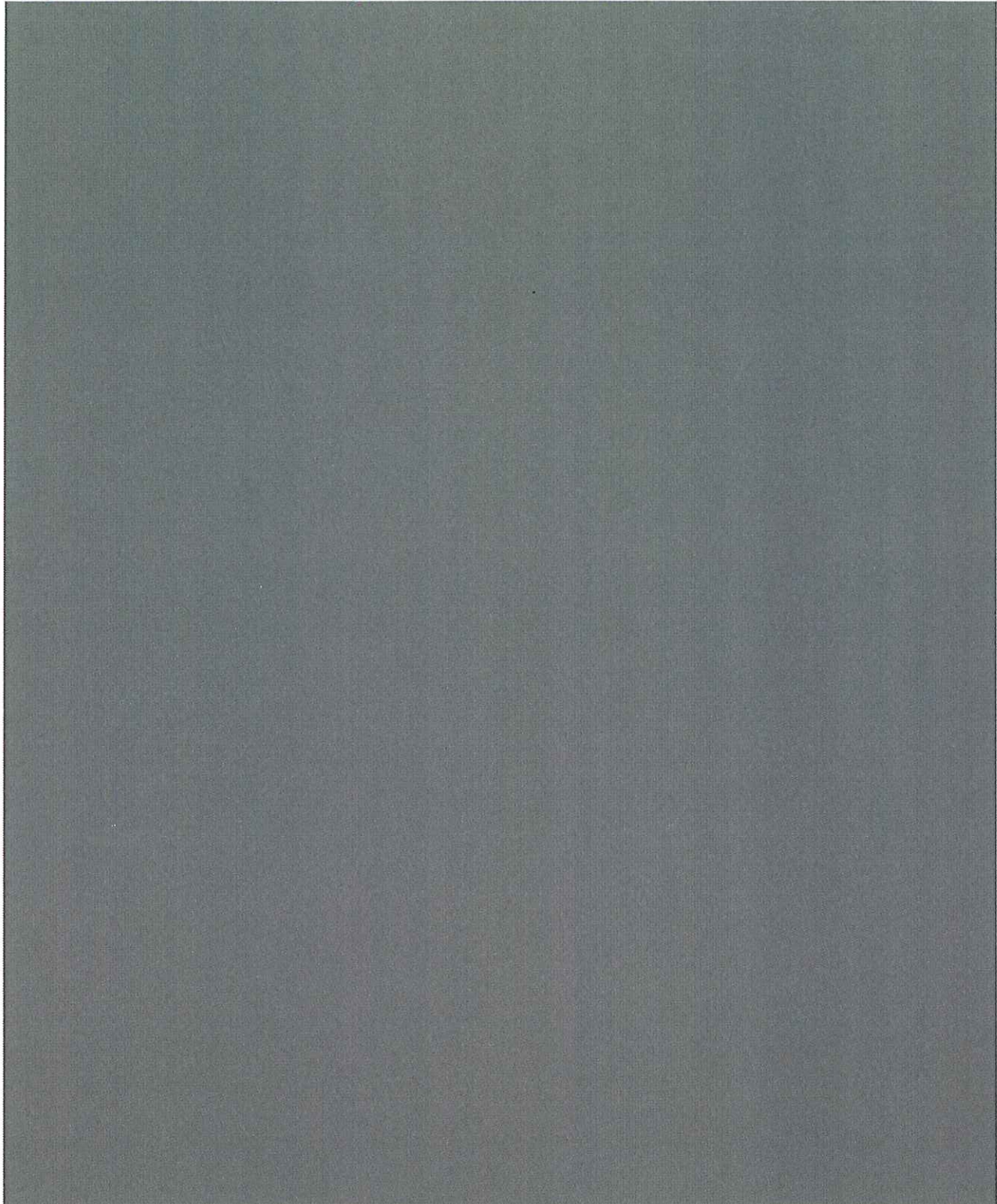
~~SENSITIVE SECURITY INFORMATION~~

Go Back

Version 1

Release Date: November 13, 2019

Implementation Date: Determined Locally (No Later Than December 31, 2019)



~~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 PENALTIES OR OTHER ACTION. FOR U.S. GOVERNMENT AGENCIES, PUBLIC DISCLOSURE GOVERNED BY 5 U.S.C. 552 AND 49 CFR PARTS 15 AND 1520.

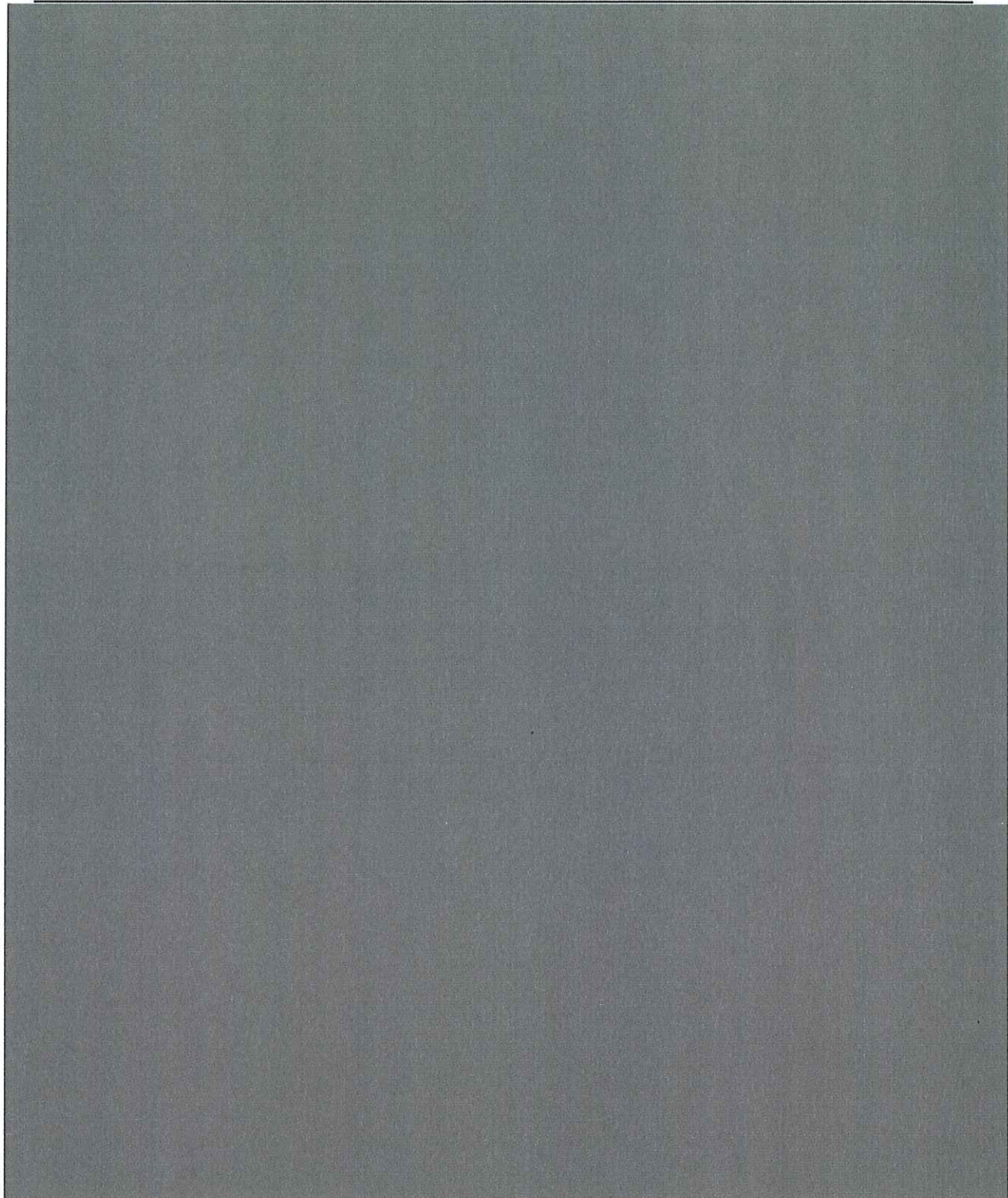
~~SENSITIVE SECURITY INFORMATION~~

Go Back

Version 1

Release Date: November 13, 2019

Implementation Date: Determined Locally (No Later Than December 31, 2019)



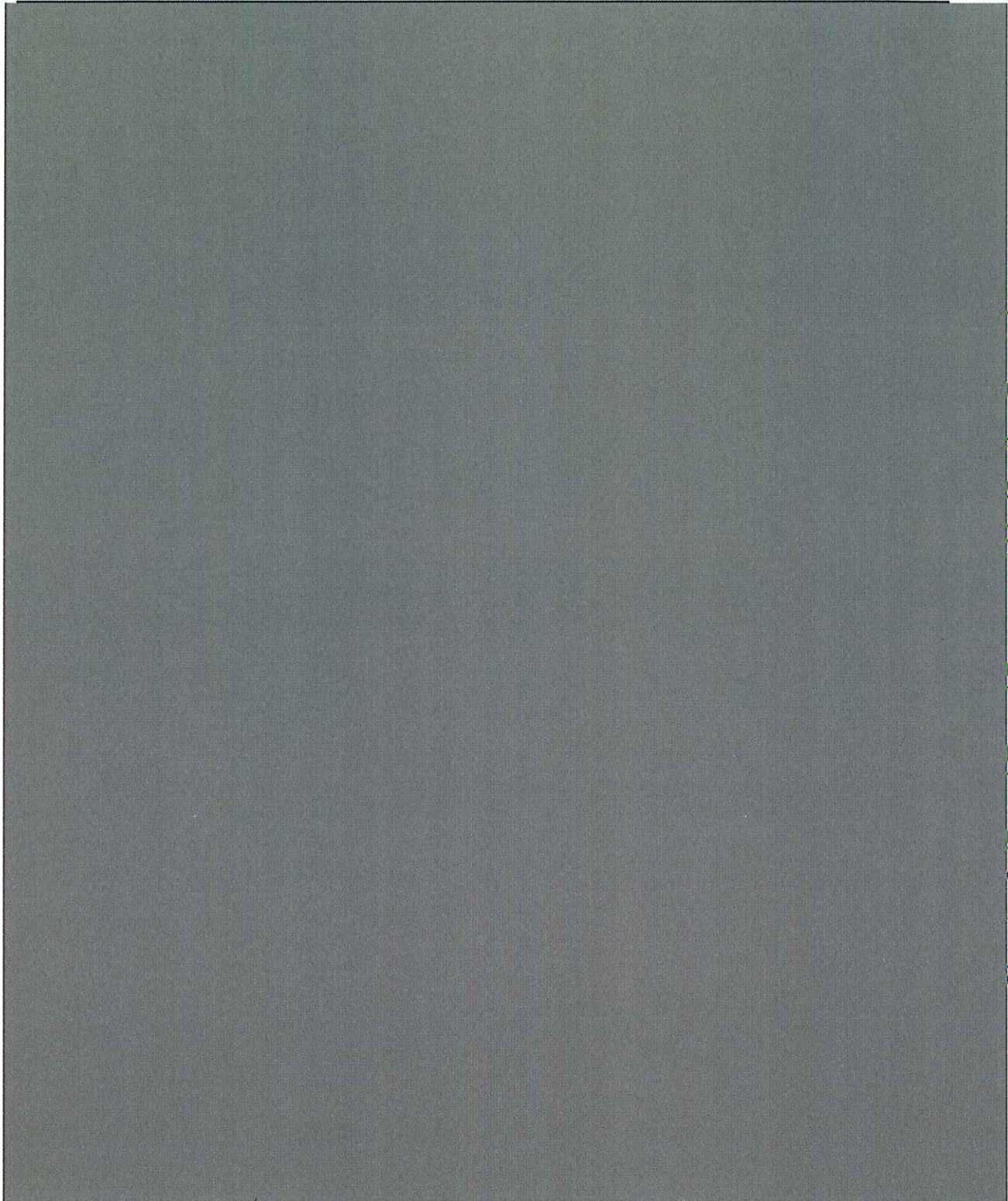
~~SENSITIVE SECURITY INFORMATION~~

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 PENALTIES OR OTHER ACTION. FOR U.S. GOVERNMENT AGENCIES, PUBLIC DISCLOSURE GOVERNED BY 5 U.S.C. 552 AND 49 CFR PARTS 15 AND 1520.

Version 1

Release Date: November 13, 2019

Implementation Date: Determined Locally (No Later Than December 31, 2019)



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 PENALTIES OR OTHER ACTION. FOR U.S. GOVERNMENT AGENCIES, PUBLIC DISCLOSURE GOVERNED BY 5 U.S.C. 552 AND 49 CFR PARTS 15 AND 1520.

Attachment C



SENSITIVE SECURITY INFORMATION

Date: November 13, 2018
To: Federal Security Directors
From: [REDACTED], Assistant Administrator of Domestic Aviation Operations
Subject: 400.5 – ROUTINE – Release of Checkpoint & Specialized Screening SOP
Cc:
Primary POC: [REDACTED]
Secondary POC: None
References: None
Attachments:

A) B) C) D) E)

Purpose:

To release a new, consolidated and streamlined Standard Operating Procedures (SOP) for screening of individuals and accessible property.

Discussion:

To improve the manner in which procedural information is conveyed, a new SOP, titled Checkpoint & Specialized Screening (CSS) SOP, has been developed and consolidates four (4) SOPs into one document:

- Screening Checkpoint SOP
- Travel Document Check SOP
- Risk-Based Security SOP
- Specialized Screening SOP

Through workforce surveys, combining these SOPs into one document was highly recommended by the field and will assist with locating procedural information more quickly. Additional key features of the CSS SOP are:

- New chapters with consolidated procedures (for example, divesting requirements, children who appear 12 years of age or under, pets and service animals, and flight crewmembers)

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

- Increased use of visual aids
- Increased use of plain language
- Hyperlinks within the electronic version
- Restructured format (position-oriented chapters)

The CSS SOP was developed with significant input from the frontline workforce (Transportation Security Officers at Southwest Florida International Airport, Miami International Airport, Phoenix Sky Harbor International Airport, and Los Angeles International Airport), the National Advisory Council, the SOP Review Committee, and the Security Procedures Engagement Advisory Council. The new document captures recommendations provided by the field and enhances their ability to navigate the SOP.

Note: The CCS SOP does not contain any new policies and procedures.

Action:

Federal Security Directors must ensure the following:

1. TSOs performing impacted functions complete the required training. Training & Development will provide additional training information in a separate communication.
2. TSOs read and understand the SOP.
3. All SOPs (hard and electronic copies) are replaced with the applicable revision and is available at all screening locations, in accordance with Operations Directive (OD) 400-18-6E: *Safeguarding SOPs and Quick Reference Guides for Screening Operations*.
4. The updated SOP must be implemented by NLT December 31, 2019.

The following documents are cancelled upon implementation of the SOP:

1. Screening Checkpoint SOP, Revision 13 Change 1
2. Risk-Based Security SOP, Revision 2 Change 3 and Interim Change 1
3. Travel Document Check SOP, Revision 2 Change 4
4. Specialized Screening SOP, Revision 2 Change 10
5. Quick Reference Guides

Attachments:

- CSS SOP
- Non-SSI Job Aids (Prohibited/Permitted Items List & HAZMAT Discovery)
- Canine Enhanced Screening SOP
- CSS SOP Frequently Asked Questions

For questions or comments, please reach out to the POC listed above.

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.