

# TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION



## **Controls Over the Management and Security of Official Passports Need Improvement**

August 26, 2020

Reference Number: 2020-10-051

TIGTACommunications@tigta.treas.gov | [www.treasury.gov/tigta](http://www.treasury.gov/tigta) | 202-622-6500

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

To report fraud, waste, or abuse, please call us at 1-800-366-4484

## HIGHLIGHTS: Controls Over the Management and Security of Official Passports Need Improvement



Final Audit Report issued on August 26, 2020  
Reference Number 2020-10-051

### Why TIGTA Did This Audit

This audit was initiated to evaluate IRS compliance with Federal requirements for management and security of official and diplomatic Government passports issued to IRS employees and appointees.

#### Impact on Taxpayers

The IRS has issued more than 2,500 official and diplomatic passports to its employees. Taxpayers have an interest in knowing that the IRS has effective security over the handling and storage of official and diplomatic passports to limit the potential of such sensitive items being stolen or misplaced and subsequently used for identity impersonation. Similarly, delayed return of official passports used for international travel increases the risk of those passports being misplaced or lost. Further, retaining passports and travel records when no longer needed increases the risk of exposing sensitive employee personal information to fraudulent use.



If lost or stolen, passports can be used by identity thieves to impersonate IRS employees.



### What TIGTA Found

IRS controls over management and security of official passports need improvement. TIGTA reviewed a statistical sample of 133 official and diplomatic passports maintained by the three international travel offices responsible for managing and securing those passports. Our review identified that controls need to be strengthened for the timely return and tracking of passports used for international travel, disposal of passport and travel records when no longer needed, and security of official passport storage and access.

Within the selected sample of 133 official and diplomatic passports, 32 employees engaged in official overseas travel. In 26 of the 32 instances, either employees did not return official passports within the required time frame upon completion of travel, or the travel coordinators did not update tracking records and TIGTA was unable to determine the date the passports were returned. Further, the IRS retained expired passports and official travel records past retention requirements.

Finally, official passports were not always stored in containers meeting security requirements, and access keys to official passport storage containers were not always maintained securely. Responsible IRS staff were not aware of the security container requirements for the storage of passports. The IRS updated its procedures to clarify security requirements of passports after our initial site visits. However, due to the timing of these changes, TIGTA was unable to assess compliance with the recent updates.

### What TIGTA Recommended

TIGTA made recommendations to the Deputy Commissioner for Services and Enforcement and the Chief Counsel to formalize written procedures for designated travel office employees to follow up with travelers who have not returned passports timely and consider including a requirement for independent periodic or annual surprise security reviews of passport offices to ensure that passport personnel are adhering to updated guidelines for the security and safeguarding of passports. TIGTA also recommended that the Deputy Commissioner for Services and Enforcement ensure that related travel files and passports are not being retained beyond established time frames unless there is a legitimate business need for them.

The IRS agreed with two recommendations and plans to review and destroy travel records beyond the retention period relating to official passports and international travel, and plans to conduct periodic security reviews to ensure adherence to updated guidelines. The IRS partially agreed with one recommendation and plans to follow current follow-up procedures for the return of official passports after travel is completed. However, the IRS did not fully address the need for all travel office supervisors to review passport log records to ensure that travel dates and related passport return dates are properly recorded.



TREASURY INSPECTOR GENERAL  
FOR TAX ADMINISTRATION

**U.S. DEPARTMENT OF THE TREASURY**

**WASHINGTON, D.C. 20220**

August 26, 2020

**MEMORANDUM FOR:** COMMISSIONER OF INTERNAL REVENUE

**FROM:** Michael E. McKenney  
Deputy Inspector General for Audit

**SUBJECT:** Final Audit Report – Controls Over the Management and Security of  
Official Passports Need Improvement (Audit # 201910016)

This report presents the results of our review to evaluate Internal Revenue Service (IRS) compliance with Federal requirements for management and security of official and diplomatic Government passports issued to IRS employees and appointees as of March 31, 2019. This review is included in our Fiscal Year 2020 Annual Audit Plan and addresses the major management and performance challenge of *Security Over Taxpayer Data and Protection of IRS Resources*.

Management's complete response to the draft report is included as Appendix II.

Copies of this report are also being sent to the IRS managers affected by the report recommendations. If you have any questions, please contact me or Heather M. Hill, Assistant Inspector General for Audit (Management Services and Exempt Organizations).



## Controls Over the Management and Security of Official Passports Need Improvement

---

### Table of Contents

<b>Background</b>	Page 1
<b>Results of Review</b>	Page 2
<u>Controls Over the Timely Return and Tracking of     Passports Used for International Travel Should Be     Strengthened</u>	Page 3
<u>Recommendation 1:</u>	Page 4
<u>Passport and Travel Records Should Be Disposed of     When No Longer Needed</u>	Page 4
<u>Recommendation 2:</u>	Page 5
<u>Security Over Official Passport Storage and Access Needs     Improvement</u>	Page 5
<u>Recommendation 3:</u>	Page 6
<b>Appendices</b>	
<u>Appendix I – Detailed Objective, Scope, and Methodology</u>	Page 7
<u>Appendix II – Management’s Response to the Draft Report</u>	Page 9
<u>Appendix III – Abbreviations</u>	Page 15



## Controls Over the Management and Security of Official Passports Need Improvement

### Background

The U.S. passport is a travel document issued under the authority of the Secretary of State attesting to the identity and nationality of the bearer. The Department of State issues official and diplomatic passports to individuals representing or conducting business on behalf of the Federal Government. Specifically:

- Diplomatic passports are issued to individuals with diplomatic status either because of performing diplomatic duties on behalf of the U.S. Government or because of the office held. The Internal Revenue Manual (IRM) requires diplomatic passports for the top management positions of each Internal Revenue Service (IRS) overseas post.<sup>1</sup> A diplomatic passport is valid for five years from the date of issue or as long as the bearer maintains his or her official status, whichever is shorter. As of March 31, 2019, the IRS had 61 active diplomatic passports on record.
- Official passports are issued to officials or employees of the U.S. Government traveling abroad on official duty. An official passport is valid for five years from the date of issue or as long as the bearer maintains his or her official status, whichever is shorter. As of March 31, 2019, the IRS had 1,133 active official passports on record.



As of March 31, 2019 the IRS had  
**61** active diplomatic passports and  
**1,133** active official passports.

An official or diplomatic passport remains the property of the U.S. Government, may only be used for official business, and must be returned upon demand. When Federal employees are required to travel internationally in support of Federal activities, they are required to apply for, possess, and display an official or diplomatic passport. To manage the official and diplomatic passports issued to IRS employees traveling on official Government business to any foreign country, the IRS maintains international travel offices with assigned travel coordinators in the Office of Chief Counsel, Criminal Investigation (CI), and Large Business and International (LB&I) Division business units. Travel coordinators in these offices are responsible for:

- Obtaining, renewing, and tracking official and diplomatic passports.
- Providing guidance on passports and other related information to travelers.
- Coordinating with a courier service for passport delivery to foreign embassies and the Department of State.
- Updating the IRS's Passport Tracker System, as applicable.

The LB&I Division travel office uses the Passport Tracker System to monitor passport activities for the majority of IRS employees.<sup>2</sup> This system is a SharePoint-driven database that maintains official and diplomatic passport information and related travel records. The Passport Tracker

<sup>1</sup> IRM 1.32.5.4.5(1), *Diplomatic Passport* (Oct. 28, 2019).

<sup>2</sup> Office of Chief Counsel employees are not tracked on the Passport Tracker System. CI employees are entered into the Passport Tracker System when the passport is initially received, but supplemental updates are not made in the system.



## Controls Over the Management and Security of Official Passports Need Improvement

System also maintains travel logs, which include details of travel such as Form 1321, *Authorization for Official Travel*, approval dates, electronic country clearance approval dates, and specific dates and destinations of travel. The database can also be used to generate reports such as expiring passports, which allows travel office coordinators to notify travelers to start the passport renewal process. In addition to the Passport Tracker System, CI tracks passports issued to its employees in a manual-entry database.<sup>3</sup> The Office of Chief Counsel also tracks passports issued to its employees separately, using a manual-entry database.

## Results of Review

IRS controls over the management and security of official passports need improvement. Our review of a statistical sample of 133 official and diplomatic passports identified that:<sup>4</sup>

- IRS employees did not always return official passports within required time frames upon completion of travel. Moreover, travel coordinators did not always update tracking records, and we were therefore unable to determine whether passports without documentation of return dates were actually returned timely.
- Passport and travel records were not disposed of when no longer needed.
- Official passports were not always stored in containers meeting security standards, and access keys to official storage containers were not always maintained securely.

 **TIGTA reviewed 133 passports and found several issues concerning the management and security of passports.**



Passports were not returned within required timeframes.



Passports and travel records were not disposed of when no longer needed.



Passports were not stored in secure containers and access keys were not secured.

During the course of our review, the IRS revised its policies to clarify passport security measures. We believe that these policy changes may resolve some security control weaknesses identified. However, these policy changes occurred subsequent to our site visits, and thus, we were unable to assess the effectiveness of the updated policies.

<sup>3</sup> Official passports issued to IRS employees acting in undercover capacities that are not tracked through the IRS Passport Tracker system, the CI and/or Office of Chief Counsel manual-entry systems are not included in this review.

<sup>4</sup> We reviewed passports maintained by the three international travel offices responsible for managing and securing official and diplomatic passports. We selected a statistical sample using a confidence level of 90 percent, an expected error rate of 15 percent, and a precision factor of  $\pm 5$  percent. We used a stratified sampling technique to evaluate 133 passports; this included active and expired passports. We selected 31 passports from the LB&I Division, 91 passports from CI, and 11 passports from the Office of Chief Counsel.



## Controls Over the Management and Security of Official Passports Need Improvement

### Controls Over the Timely Return and Tracking of Passports Used for International Travel Should Be Strengthened

Based on our analysis of IRS records, we identified 2,501 official and diplomatic passports issued to employees and appointees as of March 31, 2019.<sup>5</sup> Of the 133 official and diplomatic passports reviewed, 101 passports were associated with employees who did not perform international travel during the period covered by our review.<sup>6</sup> Of the remaining 32 passports, we determined that, in 26 instances, either the employee did not return the official passport within the required time frame upon completion of travel or the travel coordinators did not update tracking records and we were therefore unable to determine if the passports were returned timely. Specifically:

- 9 passports were not returned timely.
- 17 passports did not have associated information to determine when the passport was returned.



The IRM states that official passports should be returned by employees to the applicable travel office within ten days of the completion of international travel.<sup>7</sup> Official passports are stored at the travel office until official travel is required. Part of the travel office's responsibilities are to track official and diplomatic passports, record when employees checked out and returned passports back to the travel office, and maintain the travel files. Maintenance of the travel files includes retaining e-mail correspondence reminding employees that their passports will expire within six months and documentation that supports the return of canceled or expired passports to the Department of State.

The IRS uses a manual process to track official passport use and returns. Designated IRS travel office employees typically track passport use by recording the date official passports are issued to, and returned by, travelers on index cards stored with the official passport. Additionally, travel office employees within the LB&I Division manually update this information in the Passport Tracker System. However, we found that travel coordinators were not following the manual process to update the records, and we were therefore unable to determine the date the passports were returned, including three instances in which the travel coordinators did not capture the employees' travel dates or when the passports were returned.

IRS officials stated that, when travelers receive their official passports, they are notified that the passports must be returned within ten days of returning from travel. The three travel offices in our review stated that they have a policy for designated employees to follow up with travelers who have not returned their official passports within the required time. However, only two travel offices provided documentation of follow-up procedures. Further, those follow-up procedures have not been formally established in written guidelines such as the IRM, which provides specific instructions to responsible travel offices employees over the use and return of official passports.

<sup>5</sup> Diplomatic passports may also be issued to family members stationed overseas with the IRS employee.

<sup>6</sup> The 101 employees included employees who did not perform international travel, who were permanently overseas and not required to return their passports, or whose passports and related travel documentation were unavailable for our review due to their separation from the IRS and related return of the passports to the Department of State.

<sup>7</sup> IRM 1.32.5.4(3), *Official and Diplomatic Passports* (Oct. 28, 2019).





## Controls Over the Management and Security of Official Passports Need Improvement

The IRS also does not have guidance to instruct designated travel office employees to timely record when official passports are issued to employees and returned after overseas travel. Because there was no recording of when the passports were returned, we were unable to assess this issue. Without accurate tracking and timely follow-up on unreturned official passports, there is an increased risk of passports being stolen or misplaced.

**Recommendation 1:** The Deputy Commissioner for Services and Enforcement and the Chief Counsel should formalize written procedures for designated travel office employees to follow up with travelers who have not returned their passports in a timely manner, and for travel office supervisors to review passport log records periodically to ensure that travel dates and related passport return dates are properly recorded.

**Management's Response:** The IRS partially agreed with this recommendation. The IRS addressed the need for written procedures to follow up with travelers by stating some travel office employees will follow current follow-up procedures for the return of official passports after travel is completed, and one travel office will confirm these procedures are formalized. In addition, some travelers will be permitted to maintain custody of their official passports following the completion of international travel. The custody of those official passports will be verified on an annual basis via a 100 percent inventory review.

**Office of Audit Comment:** The IRS did not fully address the need for all travel office supervisors to review passport log records to ensure that travel dates and related passport return dates are properly recorded. Most passport documentation we reviewed did not have associated information available to determine when the passport was issued or returned. As a result, we continue to believe that supervisory review is an important element to ensure accurate official passport-related recordkeeping.

## Passport and Travel Records Should Be Disposed of When No Longer Needed

The IRS retained passports and travel records past retention requirements. Our sample of 133 passports included active and expired official and diplomatic passports issued to IRS employees. We performed a site visit to each of the three IRS travel offices responsible for securely storing official passports while not in use and found that 12 expired official passports were still being stored in the IRS travel offices despite the associated employee having separated from the IRS. The National Archive and Records Administration's General Records Schedule, dated December 2017, requires that official passports be returned to the Department of State upon the employees' separation. The 12 official passports were retained onsite from a range of 14 months to nine years past separation. IRS procedures do not include specific instructions on the process of returning expired official passports to the Department of State or maintaining documentation of such returns.



We also found that the IRS is not disposing of all official employee travel records in a timely manner. For example, at one of the international travel offices we visited, we observed travel authorizations and visa applications that



**Retaining records longer than required exposes sensitive employee personal information to fraudulent use.**





## Controls Over the Management and Security of Official Passports Need Improvement

dated back to Fiscal Year 2013.<sup>8</sup> The National Archive and Records Administration's General Records Schedule states that records related to official and diplomatic passports should be destroyed after three years unless required for business use.<sup>9</sup> Onsite officials responsible for passport recordkeeping were not aware of these records management requirements. Further, only one travel office receives biannual training specifically focused on passport processing and security through the Department of State. Designated employees in the other two travel offices receive standard IRS training covering issues such as handling sensitive materials and materials containing personal information. However, this standard training does not contain specific instructions covering the proper methods of securing passports or maintaining travel records.

Retaining outdated records beyond official use may increase the risk of exposing sensitive employee personal information to fraudulent use.

**Recommendation 2:** The Deputy Commissioner for Services and Enforcement should ensure that related travel files and passports are not being retained beyond established time frames unless there is a legitimate business need for them.

**Management's Response:** The IRS agreed with this recommendation. The IRS plans to review and destroy records that are beyond the retention period relating to official passports and international travel.

## Security Over Official Passport Storage and Access Needs Improvement

We conducted site visits to the three international travel offices responsible for maintaining and securing official passports when not in use by the traveler. These site visits included an observation of the security environment related to the storage of the passports and identified two key issues.

- In one of the three travel offices, official passports were not retained in a container that met the security requirements outlined in the IRM. The responsible business unit retained passports in an unmounted small portable box that was made of hard plastic instead of a lockable metal container.
- In two travel offices, passport personnel did not always properly secure the keys, used to access the security cabinets containing passports, from public view and exposure. During our visits to these two offices, we observed that designated personnel kept their access keys on a hook on the wall above their desks rather than maintaining physical possession of the access keys or storing the keys in a secured drawer.



The IRS established guidelines for protecting data and items that require safeguarding by the IRS.<sup>10</sup> Identification media, such as SmartID cards, pocket commissions, and passports, not in the possession of the employee must be stored in a security container or an area where only

<sup>8</sup> Any yearly accounting period, regardless of its relationship to a calendar year. The Federal Government's fiscal year begins on October 1 and ends on September 30.

<sup>9</sup> These records relate to administering the application or renewal of official passports and visas, including copies of passport and visa applications, passport and visa requests, special invitation letters, visa authorization numbers, courier receipts, and copies of travel authorizations.

<sup>10</sup> IRM 10.2.15.1 (1-2); 10.2.15.2 (1.c); 10.2.15-2, Minimum Protection Standards (Aug. 16, 2019).



## Controls Over the Management and Security of Official Passports Need Improvement

authorized persons with an official need are permitted. According to these procedures, passports should be held in a lockable metal container that has been tested for resistance to penetration, is approved for storage of high-security items, and is properly mounted. Further, keys to any room, area, secured area, or security container are also required to be safeguarded.<sup>11</sup>

At the time of our visit, the IRM that establishes standards for safeguarding IRS data and materials did not specifically address requirements for passports. Responsible IRS staff were not aware of the security container requirements for the storage of passports. Further, periodic reviews of the security environment related to passport storage did not take place to ensure adherence to IRM requirements. The IRS has established minimum security standards and requirements for which IRS managers are responsible. These procedures also require managers to ensure that the physical security measures required for protecting life, information, property, and all Government assets are applied within their area of supervision and that those measures meet the established minimum security standards. Requirements also state that periodic assessments and reviews assist security personnel and management officials in determining the effectiveness and appropriateness of existing safeguards and security guidelines.

Although our initial site visits identified needed improvements over securing passports, the IRS has taken steps to update its guidance to ensure that personnel adhere to minimum security requirements for storing and safeguarding passports. Specifically, these updated procedures now include passports as an official form of media identification, link passports directly to detailed minimum protection standards for protecting items and data that require safeguarding, and include methods of providing protection for various items (including keys and security containers).

Because the IRS revised its procedures to clarify security requirements for passports subsequent to our initial site visit, we were unable to assess IRS compliance with those recent updates.

**Recommendation 3:** The Deputy Commissioner for Services and Enforcement and the Chief Counsel should consider including a requirement for independent periodic or annual surprise security reviews of the passport offices to ensure that passport personnel are adhering to updated guidelines for securing and safeguarding passports.

**Management's Response:** The IRS agreed with this recommendation. The IRS plans to conduct periodic reviews to ensure adherence to updated guidelines.

<sup>11</sup> IRM 1.4.6.1.3 (4), *Resources Guide For Managers, Managers Security Handbook* (May 4, 2020)



## Controls Over the Management and Security of Official Passports Need Improvement

# Appendix I

### Detailed Objective, Scope, and Methodology

Our overall objective was to evaluate IRS compliance with Federal requirements for management and security of official and diplomatic Government passports issued to IRS employees and appointees as of March 31, 2019. To achieve our objective, we:

- Identified and reviewed relevant laws, regulations, policies, and procedures regarding the IRS's management and security of official and diplomatic passports.
- Determined whether the IRS effectively and consistently tracked official and diplomatic passports.
- Conducted site visits to the three international travel offices responsible for securing official passports and determined whether passports were stored in accordance with passport security requirements.
- Selected a stratified random sample of official and diplomatic passports and conducted site visits to IRS international travel office locations to determine whether the sampled passports were stored onsite, as required, within 10 days of the last passport holder's travel event. We grouped official and diplomatic passports into three strata representing each IRS business unit with an international travel office (LB&I Division, Office of Chief Counsel, and CI). We selected a statistically valid sample of 133 of the 2,501 official and diplomatic passports based on input from the contracted statistician. The sample size was based on a 90 percent confidence interval, a 15 percent expected error rate, and a  $\pm 5$  percent precision rate. We chose a statistical random sample to ensure that all passports in our population had an equal chance of being selected and to allow the results to be projected to the overall population. For all passports not present at IRS travel office locations, we determined whether the IRS had sufficient documentation to justify the absence of the passport. The contracted statistician assisted with the development of the sampling plan.
- Determined whether the IRS is compliant with Federal requirements and regulations associated with the security of official and diplomatic passports.

### Performance of This Review

This review was performed at the IRS National Headquarters in Washington, D.C., and included work in the LB&I Division's Travel Office and Visitors Program, the Office of the Deputy Chief Counsel (Operations); and CI's International Operations during the period of May through December 2019. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Major contributors to the report were Heather M. Hill, Assistant Inspector General for Audit (Management Services and Exempt Organization); LaToya R. Penn, Director; Seth A. Siegel, Audit Manager; Gary D. Pressley, Lead Auditor; and Trisa Brewer, Senior Auditor.



## **Controls Over the Management and Security of Official Passports Need Improvement**

---

### **Validity and Reliability of Data From Computer-Based Systems**

We assessed the reliability of the passport data obtained by performing electronic testing of data elements, reviewing existing information about the data and the system that produced them, and interviewing agency officials knowledgeable about the data. We determined that the data were sufficiently reliable for the purposes of this report.

### **Internal Controls Methodology**

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: LB&I Division, Office of Chief Counsel, and CI policies and procedures related to the review and approval of official and diplomatic passports. To assess these controls, we selected and reviewed a statistically valid random sample of official and diplomatic passports recorded on IRS listings and conducted site visits to IRS international travel office locations.



## Controls Over the Management and Security of Official Passports Need Improvement

## Appendix II

### Management's Response to the Draft Report



COMMISSIONER  
LARGE BUSINESS AND  
INTERNATIONAL DIVISION

DEPARTMENT OF THE TREASURY  
INTERNAL REVENUE SERVICE  
WASHINGTON, DC 20224

July 21, 2020

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT  
MICHAEL E. MCKENNEY

FROM: Douglas W. O'Donnell  
Commissioner, Large Business and International Division

Digitally signed by Douglas W.  
O'Donnell  
Date: 2020.07.21 14:38:14 -04'00'

SUBJECT: Draft Audit Report - Controls Over the Management and Security  
of Official Passports Need Improvement (Audit 201910016)

Thank you for the opportunity to review and comment on the above referenced draft audit report. We appreciate your acknowledgement of our efforts to ensure compliance with the Federal requirements for passport management and security of official Government passports issued to IRS employees.

When Federal employees are required to travel internationally on behalf of the United States Government, they are required to utilize an official or diplomatic passport. To effectively manage official or diplomatic passports issued to employees in support of Federal activities, the IRS maintains dedicated offices with assigned coordinators in the Office of Chief Counsel, Criminal Investigation (CI), and Large Business & International Division (LB&I).

The IRS takes seriously our responsibility to ensure that all official passports are handled, processed, and stored with the highest levels of security in mind. We are committed to adhering to all policies, procedures, and guidelines that are applicable to our passport management system. Indeed, we recently revised our security policy for the safekeeping of passports, and our implementation of your recommendations will further strengthen the controls over this process.

If you have any questions, please contact me, or a member of your staff may contact Keith Henley, Director, Program & Business Solutions at 205-532-4101.

Attachment



## Controls Over the Management and Security of Official Passports Need Improvement

---

Attachment

### Large Business & International Division:

#### **RECOMMENDATION 1**

The Deputy Commissioner for Services and Enforcement and the Chief Counsel should formalize written procedures for designated travel office employees to follow up with travelers who have not returned their passports in a timely manner and for travel office supervisors to review passport log records periodically to ensure that travel dates and related passport return dates are properly recorded.

#### **CORRECTIVE ACTION**

The LB&I International Travel Office has procedures for issuing and requesting prompt return of official passports from travelers. Currently, an email is sent to a traveler prior to departure instructing a return of the passport within 10 days after completion of international travel. In addition, a reminder is sent out 5 days after completion of travel. If a passport is not returned timely, an additional email is sent out with instructions to the traveler.

#### **IMPLEMENTATION DATE**

N/A

#### **RESPONSIBLE OFFICIAL**

N/A

#### **CORRECTIVE ACTION MONITORING PLAN**

N/A

#### **RECOMMENDATION 2**

The Deputy Commissioner for Services and Enforcement should ensure that related travel files and passports are not being retained beyond established time frames unless there is a legitimate business need for them.

#### **CORRECTIVE ACTION**

The LB&I International Travel Office will review and destroy records beyond the retention period relating to official passports and international travel. The Passport Tracker SharePoint site will be updated to record the date of issuance and collection of an official passport.

#### **IMPLEMENTATION DATE**

June 30, 2021

#### **RESPONSIBLE OFFICIAL**

Director, Program & Business Solutions, Large Business & International Division





## Controls Over the Management and Security of Official Passports Need Improvement

---

2

### **CORRECTIVE ACTION MONITORING PLAN**

IRS will monitor this corrective action as part of our internal management system of controls.

### **Criminal Investigation:**

#### **RECOMMENDATION 1**

The Deputy Commissioner for Services and Enforcement and the Chief Counsel should formalize written procedures for designated travel office employees to follow up with travelers who have not returned their passports in a timely manner and for travel office supervisors to review passport log records periodically to ensure that travel dates and related passport return dates are properly recorded.

#### **CORRECTIVE ACTION**

To minimize risk of loss, Criminal Investigation, Office of International Operations (CI:IO) will update the Internal Revenue Manual (IRM) 9.11.2.4.4 to reflect that custody of official Government passports are maintained in the same manner as other accountable property issued to CI employees, such as law enforcement credentials. CI will utilize its Management Information System (CIMIS) to account for the whereabouts and custody of a passport. In addition, recordation will be memorialized with a Custody Receipt for Government Property (Form 1930/EQR01).

Logs will be used to record receipt of newly issued passports and any submitted to the Travel Office for renewal or obtaining visas. CI:IO personnel will review these logs on a quarterly basis to ensure their accuracy. The new procedures will eliminate the need to return passports to Headquarters within 10 days and reduce the risk of loss from recurring mailings.

Custody of passports will be verified on an annual basis via a 100% inventory review. To further mitigate the risk of loss, a random verification of a representative sample will be conducted during bi-annual Director, Field Operations (DFO) reviews. This policy revision is modeled after TIGTA's Operations Manual Section 400 50.11.

#### **IMPLEMENTATION DATE**

November 15, 2020

#### **RESPONSIBLE OFFICIAL**

Executive Director, Criminal Investigation, Office of International Operations

### **CORRECTIVE ACTION MONITORING PLAN**

IRS will monitor this corrective action as part of our internal management system of controls.





## Controls Over the Management and Security of Official Passports Need Improvement

---

3

### **RECOMMENDATION 2**

The Deputy Commissioner for Services and Enforcement should ensure that related travel files and passports are not being retained beyond established time frames unless there is a legitimate business need for them.

### **CORRECTIVE ACTION**

CI:IO will review and destroy records, on an annual basis, beyond the retention period relating to official passports and international travel. Transfer and custody of an official Government passport will be recorded on an employee's profile in CIMIS and a Custody Receipt for Government Property (Form 1930/EQR01), which will cause the passport to be listed on an employee's inventory of issued Government equipment. Consequently, a passport will be collected by an employee's supervisor at time of separation. The IRM will be updated to reflect this change and instructions will be issued to supervisors to collect and submit official passports to CI:IO for return to the Department of State.

### **IMPLEMENTATION DATE**

November 15, 2020

### **RESPONSIBLE OFFICIAL**

Executive Director, Criminal Investigation, Office of International Operations

### **CORRECTIVE ACTION MONITORING PLAN**

IRS will monitor this corrective action as part of our internal management system of controls.

### **RECOMMENDATION 3**

The Deputy Commissioner for Services and Enforcement and the Chief Counsel should consider including a requirement for independent periodic or annual surprise security reviews of the passport offices to ensure that passport personnel are adhering to updated guidelines for securing and safeguarding passports.

### **CORRECTIVE ACTION**

CI:IO will increase accountability of official passports by updating its custody and verification process. New procedures will also minimize risk of loss in mailing passports back and forth between the custodian and a traveler. Consequently, CI:IO will update IRM 9.11.2.4.4 to reflect that custody of official passports are maintained in the same manner as other accountable property, such as law enforcement credentials. Recordation of custody of a passport will be done via CIMIS and a Custody Receipt for Government Property (Form 1930/EQR01). Custody of passports will be verified on an annual basis via a 100% inventory review. In addition, a random verification of a representative sample will be conducted during bi-annual area Director reviews. This policy revision is modeled after TIGTA's Operations Manual Section 400 50.11.



## Controls Over the Management and Security of Official Passports Need Improvement

---

4

### **IMPLEMENTATION DATE**

November 15, 2020

### **RESPONSIBLE OFFICIAL**

Executive Director, Criminal Investigation, Office of International Operations

### **CORRECTIVE ACTION MONITORING PLAN**

IRS will monitor this corrective action as part of our internal management system of controls.

### **Chief Counsel:**

### **RECOMMENDATION 1**

The Deputy Commissioner for Services and Enforcement and the Chief Counsel should formalize written procedures for designated travel office employees to follow up with travelers who have not returned their passports in a timely manner and for travel office supervisors to review passport log records periodically to ensure that travel dates and related passport return dates are properly recorded.

### **CORRECTIVE ACTION**

Chief Counsel, International, has formal written procedures directing foreign travelers that they must return their official passports timely, no later than two days after travel is completed, to the Travel Coordinator. The designated travel office employees have procedures in place to follow up with travelers who have not returned their passports in a timely manner, and there are also procedures in place to maintain passport log records and to ensure that the logs are accurate and maintained in a timely manner. Chief Counsel, International, will confirm that these procedures are also written and formalized.

### **IMPLEMENTATION DATE**

April 15, 2021

### **RESPONSIBLE OFFICIAL**

Deputy Associate Chief Counsel, International

### **CORRECTIVE ACTION MONITORING PLAN**

IRS will monitor this corrective action as part of our internal management system of controls.

### **RECOMMENDATION 3**

The Deputy Commissioner for Services and Enforcement and the Chief Counsel should consider including a requirement for independent periodic or annual surprise security reviews of the passport offices to ensure that passport personnel are adhering to updated guidelines for securing and safeguarding passports.



## Controls Over the Management and Security of Official Passports Need Improvement

---

5

### **CORRECTIVE ACTIONS**

Counsel will conduct periodic reviews to ensure Counsel adheres to the updated guidelines.

### **IMPLEMENTATION DATE**

April 15, 2021

### **RESPONSIBLE OFFICIAL**

Deputy Associate Chief Counsel, International

### **CORRECTIVE ACTION MONITORING PLAN**

IRS will monitor this corrective action as part of our internal management system of controls.



## Controls Over the Management and Security of Official Passports Need Improvement

---

### Appendix III

#### Abbreviations

CI	Criminal Investigation
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
LB&I	Large Business and International