TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Actions Are Needed to Improve the Safeguarding of Taxpayer Information at Volunteer Program Sites

November 13, 2019

Reference Number: 2020-40-004

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.

Redaction Legend:
2 = Law Enforcement Techniques/ Procedures and Guidelines for Law Enforcement Investigations or Prosecutions

Phone Number / 202-622-6500
E-mail Address / TIGTACommunications@tigta.treas.gov
Website / http://www.treasury.gov/tigta

To report fraud, waste, or abuse, call our toll-free hotline at:

1-800-366-4484

By Web:

www.treasury.gov/tigta/

Or Write:

Treasury Inspector General for Tax Administration
P.O. Box 589
Ben Franklin Station
Washington, D.C. 20044-0589

Information you provide is confidential and you may remain anonymous.

HIGHLIGHTS

ACTIONS ARE NEEDED TO IMPROVE THE SAFEGUARDING OF TAXPAYER INFORMATION AT VOLUNTEER PROGRAM SITES

Highlights

Final Report issued on November 13, 2019

Highlights of Reference Number: 2020-40-004 to the Commissioner of Internal Revenue.

IMPACT ON TAXPAYERS

The Volunteer Program plays an important role in helping the IRS improve taxpayer service and increase participation in the tax system. The program provides no-cost Federal tax return preparation and electronic filing to underserved segments of individual taxpayers, including low-income to moderate-income, elderly, disabled, and limited-English-proficient taxpayers. Because taxpayers who use return preparation services at volunteer sites disclose their Personally Identifiable Information and this information is coveted by identity thieves, the sites must safeguard taxpayer information.

WHY TIGTA DID THE AUDIT

Security over taxpayer data and protection of resources is a top IRS management challenge. The audit was initiated to assess the adequacy of and adherence to the IRS's volunteer site requirements to safeguard and protect sensitive taxpayer information.

WHAT TIGTA FOUND

The Stakeholder Partnerships, Education, and Communication function worked with its partners to heighten awareness of data security at volunteer sites. However, improvements are needed in some areas to strengthen the data security processes. For example, the IRS's partners participating in the Volunteer Program do not develop a written Information Security Plan for each site.

TIGTA's unannounced visits to 20 volunteer sites identified multiple security weaknesses at each site, such as 1) ************2****************
***************************2***************************
*****2*****, 2) site coordinators are unaware of security requirements, 3) sites using wireless connections to transmit taxpayer data did not complete a required risk assessment, and 4) ***********************2***************************
*******2******.

Finally, TIGTA found that procedures should be improved to reduce the risk of potential identity theft. *******************2*************************
***************************2***************************
***************************2***************************
***************************2***************************
***************************2***************************
***************************2***************************
***************************2***************************
*******2******.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the IRS 1) issue guidance to its partners requiring them to develop an information security plan for each site; 2) require site coordinators to use the security feature included in the tax preparation software to restrict volunteers' access to prepared returns; 3) develop procedures to confirm that site coordinators are aware of security requirements; 4) ensure that site reviews include an assessment of compliance with security controls; 5) update procedures for partners to validate volunteers' identity using only Government-issued identification prior to participating in the Volunteer Program; 6) reinforce training for Stakeholder Partnerships, Education, and Communication function reviewers and site coordinators on how to report volunteers who are caught violating the standards of conduct; 7) develop procedures to evaluate security incidents at Volunteer Program sites to identify affected taxpayers whose information is at risk; and 8) emphasize to all volunteer sites and partners their responsibilities to evaluate and report to the IRS all partner-owned and IRS-loaned lost or stolen computers.

IRS management agreed with the recommendations and plans to take corrective actions.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

November 13, 2019

MEMORANDUM FOR COMMISSIONER OF INTERNAL REVENUE

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Actions Are Needed to Improve the Safeguarding of Taxpayer Information at Volunteer Program Sites (Audit # 201840010)

This report presents the results of our review to assess the adequacy of and adherence to the Internal Revenue Service's (IRS) volunteer site requirements to safeguard and protect sensitive taxpayer information. This review was part of our Fiscal Year 2019 Annual Audit Plan and addresses the major management challenges of Security Over Taxpayer Data and Protection of IRS Resources.

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

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 Russell P. Martin, Assistant Inspector General for Audit (Returns Processing and Account Services).

Table of Contents

Abbreviations

DSL	Dynamic Selection List
FY	Fiscal Year
IRS	Internal Revenue Service
SPEC	Stakeholder Partnerships, Education, and Communication
SSN	Social Security Number
TIGTA	Treasury Inspector General for Tax Administration
TIN	Taxpayer Identification Number

Background

The Volunteer Program plays an important role in helping the Internal Revenue Service (IRS) improve taxpayer service and increase participation in the tax system. The program provides no-cost Federal tax return preparation and electronic filing to underserved segments of individual taxpayers, including low- to moderate-income, elderly, disabled, and limited-English-proficient taxpayers. The Volunteer Program includes the Volunteer Income Tax Assistance and the Tax Counseling for the Elderly programs and sites operated in partnership with the U.S. military and community-based organizations.[1] The program is managed by the IRS's Stakeholder Partnerships, Education, and Communication (SPEC) function.[2] Figure 1 provides the number of Volunteer Program tax return preparation sites, volunteers, and returns prepared during Fiscal Years (FY) 2017 through 2019.

Figure 1: Volunteer Program Trends for FY 2017 Through FY 2019

Fiscal Year	Number of Volunteer Sites	Number of Volunteers	Tax Returns Prepared
2017	11,469	87,214	3,558,491
2018	11,044	84,646	3,559,838
2019	10,921	82,214	3,458,737[3]

Source: SPEC function website and IRS management.

Volunteer requirements to enroll, participate, and prepare tax returns

The IRS requires volunteers to meet certain requirements before they can participate in the Volunteer Program. The IRS indicates that these requirements help ensure that volunteers maintain the greatest degree of public trust and the highest standards of ethical conduct. Requirements include:

- Completing a registration process in which the volunteer provides his or her name and address along with a photo identification card such as a driver's license to a Volunteer Program partner for use in verifying the volunteer's identity.
- Completing the Volunteer Standards of Conduct training, which is mandatory for new volunteers and discretionary for returning volunteers. This training includes an

[1] Community-based organizations may include colleges, senior citizen centers, faith-based organizations, and libraries.
[2] The SPEC function is in the Wage and Investment Division.
[3] As of April 28, 2019.

explanation of the Volunteer Program's six standards of conduct (see Figure 2), information on how to report possible violations, and consequences of failure to adhere to the program requirements. In addition, all volunteers must pass a Volunteer Standards of Conduct test prior to volunteering at a site.

- Passing a mandatory tax knowledge test (new and returning volunteers). Requiring a volunteer to pass this test is an effort to ensure that tax returns are prepared accurately and tax laws are applied correctly.
- Signing and dating Form 13615, *The Volunteer Standards of Conduct Agreement*, agreeing to follow the Volunteer Standards of Conduct. Figure 2 is an excerpt from Form 13615 that outlines these standards.

Figure 2: Form 13615 Standards of Conduct

Standards of Conduct: As a volunteer in the VITA/TCE Programs, you must:

1) Follow the Quality Site Requirements (QSR).	4) Not knowingly prepare false returns.
2) Not accept payment, solicit donations, or accept refund payments for federal or state tax return preparation from customers.	5) Not engage in criminal, infamous, dishonest, notoriously disgraceful conduct, or any other conduct deemed to have a negative effect on the VITA/TCE Programs.
3) Not solicit business from taxpayers you assist or use the knowledge you gained (their information) about them for any direct or indirect personal benefit for you or any other specific individual.	6) Treat all taxpayers in a professional, courteous, and respectful manner.

Source: Excerpt from IRS Form 13615. VITA = Volunteer Income Tax Assistance. TCE = Tax Counseling for the Elderly.

Registry of volunteers permanently barred from participating in the Volunteer Program

The SPEC function maintains a Volunteer Registry of individuals permanently barred from participating in the Volunteer Program. This registry is a cumulative list of volunteers that site coordinators, SPEC function employees, and taxpayers reported to the SPEC function for violating one or more of the Standards of Conduct. IRS guidance states that SPEC function territory managers must review the registry and compare it to the annual volunteer lists such as Form 13533, *Sponsor Agreements*, or Form 13206, *Volunteer Assistance Summary Reports.* If a volunteer's name appears on the registry, the SPEC function territory manager must advise the partner or volunteer that they cannot participate in the program. If another attempt is made to participate, the territory manager must notify the Treasury Inspector General for Tax Administration (TIGTA) Office of Investigations.

As of March 20, 2019, the Registry included 62 individuals, of which 16 were added in Calendar Years 2016 through 2019. Figure 3 details the violations committed by the 16 individuals.

Figure 3: Volunteers Added to the Volunteer Registry in Calendar Years 2016–2019

Calendar Year	Number of Volunteers	Reasons for Adding the Volunteer to the Registry
2016	5	1 – Refused to wear ID badge. 1 – Took documents home to prepare out-of-scope returns. 1 – Knowingly prepared false tax returns. 1 – Knowingly prepared out-of-scope returns and accepted payments. 1 – Knowingly prepared false tax returns and deposited refunds into another account.
2017	7	2 – Knowingly prepared false tax returns. 1 – Unauthorized use of an Electronic Filing Identification Number[4] and Site Identification Number.[5] 1 – Accepted payment for tax return preparation 1 – Failure to follow Intake/Interview and Quality Review Process.[6] 2 – Engaged in criminal and dishonest conduct.
2018	3	2 – Knowingly prepared false tax returns. 1 – Engaged in criminal and dishonest conduct.
2019	1	1 – Engaged in criminal, infamous, dishonest, notoriously disgraceful, or any other conduct deemed to have a negative effect on the Volunteer Program.

Source: SPEC function Volunteer Registry as a March 20, 2019.

[4] Providers need an IRS-assigned Electronic Filing Identification Number to electronically file tax returns.
[5] The IRS assigns a unique eight-digit Site Identification Number to each Volunteer Program site to help administer the program.
[6] Process of completing the Form 13614-C, *Intake/Interview & Quality Review Sheet*, and interviewing the taxpayer to ensure that volunteers obtain the necessary information and prepare an accurate tax return.

Publication 4299, Privacy, Confidentiality, and Civil Rights, outlines volunteer site requirements to protect taxpayer information

Publication 4299 provides information on the requirements that volunteers must follow to protect taxpayer information. Volunteer sites are required to maintain a copy of Publication 4299 for reference. In addition to Publication 4299, the SPEC function holds monthly web conferences with volunteers to discuss current topics and may use this forum to discuss any security issues that may surface. Figure 4 details the requirements listed in Publication 4299 that sites must follow in an effort to protect taxpayer information.

Figure 4: Requirements to Safeguard Taxpayer Information

Publication 4299 Requirement	Publication 4299 Description
Privacy During the Interview	To the extent possible, arrange tax preparation assistance areas to prevent others from easily overhearing or viewing the information under discussion.
Requesting Taxpayer Information	When preparing tax returns, only information (*i.e.*, Social Security Number (SSN), birth dates, bank account information) that is necessary and relevant should be requested. The information provided is entrusted to the volunteer with the taxpayer's confidence that it will not be shared or used in any unauthorized manner.
Validating Taxpayer's Identity and Identification Numbers	Volunteers preparing tax returns must confirm the identity of each taxpayer signing the tax return to prevent identity theft and tax fraud. The volunteer must review an original photo identification such as valid driver's license.
Signing the Tax Return	A taxpayer must sign the tax return, whether paper-filed or Form 8879, *IRS e-file Signature Authorization*, for an electronically filed tax return.
Sharing the Information	Information provided for tax return preparation should not be shared with anyone who does not have a need to know. Individuals have a need to know if their involvement is required to process the information in its final disposition (*i.e.*, guidance in tax return completion, electronically transmitting the return, and reviewing a tax return and source documents).
Sharing Taxpayer Information Through Nontraditional Channels	Information sharing is normally done face-to-face at the site. However, there may be situations in which other communication channels (*i.e.*, advice from a more experienced preparer located offsite, discussing rejected returns) may be more efficient in the process of preparing and filing returns.
Taxpayer Consent	Partners are required to provide written notice to taxpayers and receive signed consent when using or disclosing taxpayer information for purposes other than preparing returns (*i.e.*, current, prior, or subsequent year returns).

Publication 4299 Requirement	Publication 4299 Description
Use of Wireless Devices	The IRS recommends that partners and volunteers use wired connections when transmitting taxpayer information via the Internet. Partners and volunteers who, after assessing their individual risks, decide to use wireless devices to transmit taxpayer information to the tax preparation software provider should, at a minimum, use certain specifications.
Protecting the Information	Once the tax return is complete and the taxpayer has left, partners and volunteers must ensure that the individual information provided during return preparation is protected.
Providing a Safe Environment for Information	Partners and volunteers must implement a process to ensure that taxpayer information is adequately protected at all times. For example, the process must: • Ensure that tax-related information provided during the course of tax return preparation is under the care of volunteers at all times and is maintained in accordance with partner security and safeguarding guidelines. • Implement password protection on computers used to prepare returns. • Sign off and lock computers when not in use and use locked storage for tax-related documents that are retained after the taxpayer leaves the site. • Dispose of tax-related information in a timely manner. • Delete taxpayer data as information may not be stored on partner-owned or IRS-loaned equipment once the filing season is completed. Guidelines also require information on computers to be deleted/wiped as part of the site closing activities. • Ensure that computers are in the control of a volunteer at all times while in use and stored in a controlled, limited-access, locked location when not in use. Record the make, model, and serial number of all computers used in the event a report of a lost or stolen computer must be made.
Reporting Stolen and Lost Computers	It is necessary to ensure that all incidents of stolen and lost computers (including partner-owned) are reported to the IRS. As a condition of computers loaned to partners from the IRS, the recipient agrees to notify the IRS within 48 hours of the incident. Partners are also requested to notify the IRS within 48 hours.

Source: IRS Publication 4299.

In addition to establishing Volunteer Program procedures and developing volunteer training, the SPEC function performs reviews to monitor volunteer compliance with site security requirements and Volunteer Standards of Conduct. These reviews assess whether sites have a process to 1) identify every volunteer who prepares, reviews, or changes returns; 2) secure and protect equipment; 3) safeguard and properly destroy taxpayer information; and 4) ensure that taxpayer consent notices are secured as appropriate. In addition, these reviews ensure that volunteers are certified in the Volunteer Standards of Conduct. Figure 5 provides the number of these reviews completed in FY 2018.

Figure 5: SPEC Site Reviews in FY 2018

Type of Site Review	Total Reviews
Quality Statistical Sample – Unannounced site visits performed by SPEC Headquarters to promote and measure compliance with Quality Site Requirements.	104
Field Site Visit – Unannounced site visits performed by SPEC field to assess site adherence to Quality Site Requirements and Volunteer Standards of Conduct.	1,556
Remote Site Review – Announced reviews performed by SPEC field via telephone to assess site adherence to Quality Site Requirements and Volunteer Standards of Conduct.	1,064

Source: TIGTA analysis of Forms 6729 and 6729-D.[7]

Procedures for identifying lost or stolen computers

Each year, the SPEC function loans computers to some volunteer sites for use in preparing tax returns. For example, for FY 2019 the IRS loaned 5,786 computers to partners. Publication 4299 includes the requirement for volunteer sites to report all incidents of stolen and lost computers to the IRS. Volunteers are required to notify the IRS within 48 hours for stolen or lost IRS-owned computers and are requested to notify the IRS within 48 hours for stolen or lost partner-owned computers. For stolen IRS computers, volunteers must notify local law enforcement immediately. The SPEC function then reports the incident to the IRS's Computer Security Incident Response Capability office, the TIGTA Office of Investigations, IRS management, and the IRS's Computer Depot located in Brookhaven, New York. In addition, volunteer sites are required to evaluate the risk associated with any loss of taxpayer information and, if warranted, notify the taxpayers.

[7] The Quality Statistical Sample reviewers use Form 6729, *QSS Site Review Sheet*, and the SPEC function officials who conduct Field Site Visits and Remote Site Reviews use Form 6729-D, *Site Review Sheet*. QSS = Quality Statistical Sample.

This review was performed at the Wage and Investment Division Headquarters in Atlanta, Georgia, during the period December 2018 through June 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. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Results of Review

Security over taxpayer data and protection of resources is a top management challenge for the IRS in FY 2019. Taxpayers who use return preparation services at volunteer sites are required to disclose sensitive Personally Identifiable Information that includes their name, address, SSN, birth date, and bank account information to a volunteer for use in preparing their tax return. This sensitive information is highly coveted by identity thieves. Thus, the IRS must implement effective procedures to ensure that the volunteer sites adequately safeguard taxpayer information. Our review identified that the SPEC function has worked with its partners to heighten awareness of data security at volunteer sites. However, improvements are needed to strengthen data security processes.

An Information Security Plan Is Not Developed for Each Volunteer Program Site

The IRS does not require its partners participating in the Volunteer Program to develop a written information security plan for each site where taxpayers are provided free tax return preparation. An information security plan is a formal document that provides an overview of the security controls in place or planned to protect taxpayer information. For example, the Federal Trade Commission's Safeguards Rule[8] requires financial institutions to develop a written information security plan that describes the program to protect customer information. The security plan must:

- Designate one or more employees to coordinate the information security program.
- Identify and assess the risks to customer information in each relevant area of its operation and evaluate the effectiveness of the safeguards for controlling these risks.
- Evaluate and adjust the tax preparation program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.

When we raised our concerns to SPEC function management, they stated that they do not believe the requirement for financial institutions to develop a written information security plan applies to its partners in the Volunteer Program. Management stated that IRS Publication 4557, *Safeguarding Taxpayer Data – A Guide for Your Business*, defines a Financial Institution covered by the Safeguards Rule as professional tax preparers, and because volunteers are not

[8] The Safeguards Rule requires financial institutions under the Federal Trade Commission's jurisdiction to have measures in place to keep customer information secure.

professional tax preparers, the Safeguards Rule does not apply. We disagree. In fact, IRS Publication 4600, *Tips for Safeguarding Taxpayer Data*, contradicts management's position. According to Publication 4600, financial institutions covered by the Safeguards Rule include return preparers, data processors, transmitters, service providers, and others who are *significantly engaged in providing financial products or services that include preparing and filing tax returns*. Volunteers are significantly engaged in preparing and filing tax returns and, as such, we believe the Safeguards Rule applies and a security plan should be developed for each site in an effort to protect taxpayer data.

Recommendation

Recommendation 1**:** The Commissioner, Wage and Investment Division, should issue guidance to Volunteer Program partners requiring the development of an information security plan for each of their sites. The guidance should detail the elements to be included in this plan and the need to review the plan with volunteers and retain the plan at the site. IRS site review procedures should also be updated to include verification of the information security plan.

> ***Management's Response:*** The IRS agreed with this recommendation and plans to update Publication 4299 to include a security plan template for site coordinators to complete and sign annually. IRS management also plans to highlight key topics from Publication 4299 during a partner Security Symposium to increase awareness among internal and external stakeholders.

Unannounced Site Visits Identify Numerous Site Security Weaknesses

Our unannounced visits to 20 judgmentally[9] selected volunteer sites during February and March 2019 identified multiple security weaknesses at each of these 20 sites. The sites we visited were also sites visited by SPEC function reviewers in Calendar Year 2018. For each of these 20 sites, the SPEC reviewers concluded that the site was fully compliant with security requirements. Examples of the security weaknesses that we identified include:

- ***IRS policies and procedures do not restrict volunteer access to tax information after returns are prepared.*** Our review identified that all volunteers who prepare returns at a site have the capability to **********2**********2**********2**********. SPEC function management did not develop a policy requiring site coordinators to restrict volunteers' access to prepared returns. The tax preparation software used by volunteer sites has a security feature that would restrict

[9] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population. The selected sites were in the three SPEC function nationwide geographically organized areas, and each prepared 400 or more tax returns in Calendar Year 2018.

volunteer access to prepared returns, *********2*********. Publication 4557 states that organizations should develop policies for whether or how employees can access customer data remotely. Management stated that there are no specific expectations for volunteers accessing tax returns after hours. Instead, management expects partners to take appropriate steps to ensure the security of taxpayer data, which may include restricting after-hours access to the data.

- ***Site coordinators are unaware of security requirements in Publication 4299.*** Site coordinators at 16 sites indicated that they were unaware of Publication 4299. The SPEC function officials do not ensure that site coordinators are aware of the security requirements contained in this publication, nor do the SPEC function's site reviews determine whether site coordinators are familiar with Publication 4299 and a copy is available for volunteers to review at the site.

- ***Sites using wireless connections to transmit taxpayer information did not complete the required risk assessment.*** Wireless connection to the Internet to prepare and transmit tax returns to the IRS was used at 11 of the 20 sites we visited. Publication 4299 requires partners to assess their individual risks before using wireless devices to transmit taxpayer information. However, for the 11 sites, the partners did not complete the required risk assessment. **********2********** **********2********** **********2**********. When we discussed this issue with the SPEC function reviewers who visited these sites during the prior year, they indicated that they did not check for these security standards even though their job aid for conducting site visits instructs them to check site compliance with Publication 4299 requirements. SPEC function management acknowledged that site reviewers are not trained to assess security requirements for a wireless network.

- ***Improper and unsecured retention of taxpayer documents occurred.*** ******2******* **********2********** **********2********** **********2********** **********2********** **********2**********. Publication 4299 requires sites to:

  - Securely store taxpayers' documents away from the flow of foot traffic, out of the reach of clients.
  - Use locked containers for printed documents containing taxpayer information during and after operating hours and shred or burn information not returned to the taxpayer. Taxpayer information may be maintained by partners until they close the site at the end of the site's operational year.

- Follow Internal Revenue Code Section 7216 procedures for securing taxpayer-signed consent forms if the partners have a need to retain and use the taxpayers' information for purposes other than return preparation.

The SPEC function's reviewers did not identify these instances of *******2******** *****2***** during their site reviews because their guidelines allow them to rely on oral statements from volunteers rather than physically observing documentation retained at the site. For example, Remote Site Reviews are conducted via telephone rather than visiting the site. **********2********** **********2********** *****2*****. For another site, the SPEC function had completed a Quality Statistical Sample review in which the reviewer relied on oral testimony from the site coordinator rather than observing the documentation at the site. Finally, at the sites where we found that volunteers took **********2**********, we found that the SPEC function reviewers did not ask the volunteers about this practice. One reviewer we interviewed acknowledged that if he or she had been aware of this practice, he or she would have rated the site as not compliant.

When security weaknesses exist at the volunteer sites, taxpayers' personal information is more susceptible to theft and misuse.

Recommendations

The Commissioner, Wage and Investment Division, should:

Recommendation 2**:** Require site coordinators to use the security feature included in the tax preparation software to restrict volunteers' access to prepared returns.

Management's Response: The IRS agreed with this recommendation and plans to emphasize to site coordinators that they must use the features of tax software that restricts volunteer access to tax returns outside of site operating hours. IRS management also plans to add a question to Form 6729 for reviewers to address this issue.

Recommendation 3: Develop processes and procedures to confirm site coordinators are aware of security requirements and hold discussions with volunteers at the sites to review these security requirements.

Management's Response: The IRS agreed with this recommendation and plans to review security requirements with site coordinators during the partner Security Symposium. IRS management also plans to implement a knowledge check for the Site Coordinator's Training to test awareness of procedures.

Recommendation 4: Ensure that site reviews include an assessment of compliance with security controls outlined in Publication 4299. This assessment should determine if the site being reviewed uses a wireless computer connection and, if so, that a required risk assessment is

completed. The assessment should also include steps to identify and verify proper storage of taxpayer information.

> ***Management's Response:*** The IRS agreed with this recommendation. IRS management plans to review the quality review series of forms and job aides to determine what additional questions should be added to address the security controls outlined in Publication 4299 during site reviews.

Improvements Are Needed to Better Protect Taxpayers From Potential Identity Theft

**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
2.

Site coordinators are unaware of their responsibility to report unscrupulous volunteers to be added to the registry and removed from the program. Our interviews with site coordinators at 17 of the 20 sites we visited found that they were unaware of the registry or procedures to add volunteers to the registry. **********2**********
**********2**********
2. Of additional concern is that our interviews with six judgmentally sampled SPEC function reviewers, who conduct site assessments, identified that they do not have a consistent understanding of the Volunteer Standards of Conduct violations that warrant referring a volunteer to the SPEC function director for addition to the registry.

Procedures are not sufficient to protect taxpayers from potential identity theft when a security incident occurs at a volunteer site

The SPEC function did not implement adequate procedures to protect taxpayers from the potential risk of identity theft when their tax information is lost in a security incident at a volunteer site. Security incidents include data breaches, lost or stolen computers, and taxpayers whose returns were prepared by volunteers who were caught violating the Volunteer Standards of Conduct. For example, the Taxpayer Identification Numbers (TIN) of taxpayers who had their returns prepared by volunteers who were caught violating the Standards of Conduct and removed from the program were not reported to the Return Integrity and Compliance Services

function for evaluation and possible addition to the Dynamic Selection List (DSL)[10] for identity theft monitoring.

**********2**********
**********2**********
**********2**********
**********2**********.

**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********.

**********2**********
**********2**********
**********2**********
**********2**********
**********2**********
**********2**********.

Under current SPEC function procedures, the TINs of the taxpayers involved in the fraudulent filing of these tax returns would not be added to the DSL to protect these individuals from the filing of fraudulent tax returns using their information. **********2**********
**********2**********
**********2******.

When we asked SPEC function management why they had not implemented procedures to add the TINs of taxpayers affected by security incidents to the DSL, they stated that no taxpayer information should be stored on a computer that is lost or stolen. However, we informed management that the volunteers have the capability to **********2**********
**********2**********
2. Thus, if a computer is lost or stolen, taxpayer information may be stored on the computer. SPEC function management then indicated they are receptive to adding the TINs of

[10] The DSL is part of the IRS's system of protective controls used to select tax returns for review by the Taxpayer Protection Program. This program contacts taxpayers who own the TINs and requests they contact the IRS to authenticate their identity before processing their returns.

taxpayers affected by security incidents to the DSL for cases in which they determine that taxpayer data have been compromised.

Sites are not complying with procedures when computers are lost or stolen

Our review identified that the required Form 13747, *Checklist for Lost/Stolen Equipment*, was not prepared for five of the 36 IRS-loaned computers that were reported as lost or stolen in Calendar Years 2016 through 2018. In addition, our review of the 19 Forms 13747 that were prepared for the remaining 31 lost or stolen computers identified that the forms lacked information that the SPEC function needed to evaluate these incidents. For example, all 19 forms had missing checklist items or a vague explanation of the incident. Information missing included details on whether a police report was filed and whether sensitive data were stored on the computer. Despite this missing information, the SPEC function concluded that none of the computers stored taxpayer information and no taxpayers needed to be notified.

IRS procedures require sites to prepare a Form 13747 to report incidents of lost or stolen equipment. Volunteer Program partners are required to provide incident information such as the computer's serial number, description of events that occurred, and the taxpayer data at risk to their local SPEC function relationship manager or territory office. The territory office must then complete an incident assessment and supporting documentation within 10 days. However, when site coordinators do not properly report to the IRS all lost or stolen computers or complete the required documentation, the risks increase to the taxpayers whose information may be stored on the computers.

For the five computers lost or stolen, SPEC function management indicated that a Form 13747 was not required for three computers because the computer was lost in transit to the tax partner and that a Form 13747 was not required for the other two computers because the computers were recovered within a week. However, we believe that a Form 13747 should have been prepared for each of these incidents.

Finally, the main reason for the insufficient reporting of lost or stolen computers is the SPEC function reviewers' and site coordinators' inadequate knowledge of the requirement to report these incidents. **********2********** **********2********** ********2*********. This may be the reason that no lost or stolen partner-owned computers were reported to the SPEC function prior to our site visits. When we brought this issue to management's attention, they stated that no taxpayer information should be stored on a computer that is lost or stolen and, as such, taxpayer data are not at risk.

Recommendations

The Commissioner, Wage and Investment Division, should:

Recommendation 5**:** Update procedures for partners to validate volunteers' identity using only Government-issued identification prior to participating in the Volunteer Program.

> ***Management's Response:*** The IRS agreed with this recommendation and plans to update its procedures to require validation of volunteers' identity using only government-issued identification prior to participation in the Volunteer Program.

Recommendation 6: Reinforce training for SPEC function reviewers and site coordinators on how to report volunteers who are caught violating the Volunteer Standards of Conduct. Site reviewers should confirm an understanding of these processes and procedures with site coordinators as part of the SPEC function's reviews. Training should also address the importance of SPEC function territory managers using the Volunteer Registry to ensure that banned volunteers do not regain entry into the program.

> ***Management's Response:*** The IRS agreed with this recommendation and plans to reinforce training for SPEC function reviewers and site coordinators on how to report volunteers who violate the Volunteer Standards of Conduct. Training will also address using the Volunteer Registry to ensure that banned volunteers do not regain entry into the program.

Recommendation 7: Develop procedures to evaluate security incidents at Volunteer Program sites to identify affected taxpayers whose information is at risk and forward their TINs to the Return Integrity and Compliance Services function for evaluation and potential inclusion on the DSL. The procedures should include steps to identify taxpayers whose returns were prepared by a volunteer who the SPEC function banned from the Volunteer Program.

> ***Management's Response:*** The IRS agreed with this recommendation and plans to implement procedures for referring TINs of potentially affected taxpayers to the DSL in consultation with the Return Integrity and Compliance Services function.

Recommendation 8: Emphasize to all volunteer sites and partners their responsibilities in Publication 4299 to evaluate and report to the IRS all partner-owned and IRS-loaned lost or stolen computers. Site reviewers should confirm the site coordinators' understanding of these procedures during the SPEC function's site reviews. In addition, when lost or stolen computers are reported, ensure that Forms 13747 are prepared and include all information needed to determine the extent to which taxpayer data may be at risk.

> ***Management's Response:*** The IRS agreed with this recommendation and plans to address the issue of reporting lost computers during the partner Security Symposium. IRS management also plans to include questions on the site coordinator knowledge check to confirm understanding of the results around lost or stolen equipment. Existing

guidelines will also be reviewed to ensure consistency in reporting IRS-loaned and partner-owned equipment that is lost or stolen. Also, Forms 13747 will be reviewed to ensure that they are correct and complete.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to assess the adequacy of and adherence to the IRS's volunteer site requirements to safeguard and protect sensitive taxpayer information. To accomplish our objective, we:

I. Determined if the SPEC function implemented sufficient controls to safeguard taxpayer data at Volunteer Program sites.

A. Compared the computer security controls that the IRS requires electronic filing providers to implement in their office to the security controls the IRS requires for Volunteer Program sites. We determined if adequate controls were in place for the Volunteer Program.

1. Reviewed the electronic filing security rules and requirements that must be followed by paid tax return preparers participating in the e-File provider Program.

2. Reviewed applicable publications and guidance to identify the requirements that must be followed by Volunteer Program sites to be accepted and maintain participation in tax preparation.

3. Interviewed responsible SPEC function officials regarding controls to safeguard taxpayer data at Volunteer Program sites and the process for volunteers to prepare and submit returns.

4. Compared the security requirements to identify inconsistencies between the programs and deficiencies in the security requirements for the Volunteer Program.

B. Assessed the Volunteer Program's exposure to the risk of unauthorized disclosure of taxpayer data.

1. Determined the adequacy and effectiveness of SPEC function reviews to ensure that Volunteer Program sites are adhering to security requirements.

a) Selected and interviewed a judgmental sample[1] of six out of the 251 SPEC function reviewers to determine the processes and procedures used to complete their reviews and whether they used the same standards to ensure the enforcement of security requirements at Volunteer Program sites.

[1] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population. The reviewers selected conducted a review of at least one of the 20 sites we visited during our review.

b) Determined the adequacy of SPEC function reviews by evaluating the Publication 4299, *Privacy, Confidentiality, and Civil Rights*, guidelines and compared them to the guidelines (*i.e.*, quality site requirements, site review checklists, and job aides) used during reviews.

2. Selected a judgmental sample[2] of 20 of the 10,921 Volunteer Program sites and interviewed the site coordinators to evaluate their understanding of data security responsibilities and the implementation of site requirements to safeguard sensitive taxpayer information.

   a) Determined if sites are required to have written security policies and procedures, including procedures for protecting taxpayer data at the site.

   b) Determined how the partners verify a volunteer's identity.

   c) Determined if the sites had knowledge of Publication 4299 data security requirements and the methods they employ to ensure site compliance with all security requirements outlined in the publication.

   d) Determined the site's risk exposure related to encryption and virus protection, the need to regularly update security software on computers, and use of wireless networks.

   e) Determined the reporting actions sites must take if they suspect a data breach or a lost or stolen computer.

   f) Determined the responsibilities related to the Volunteer Registry, including how to report a volunteer.

   g) Determined the responsibilities to protect paper copies and taxpayer information stored electronically on partner-owned and IRS-owned computers.

3. For each of the 20 sites, performed walkthroughs/site visits to determine if:

   a) Sites have a physical copy of Publication 4299 on hand.

   b) Sites have a process to identify every volunteer that prepares, reviews, or changes a tax return. This includes verifying that each volunteer has taken the appropriate training.

   c) IRS computers and paper copies of taxpayer information are locked and properly stored.

[2] The selected sites were in the three SPEC function nationwide geographically organized areas, and each prepared 400 or more tax returns in Calendar Year 2018.

d) Volunteers are permitted to store taxpayer information on computers and, if so, the impact and extent of the information.

e) IRS-loaned and partner-owned computers have adequate and updated virus protection software, data encryption software, and require complex passwords.

f) Computers that store taxpayer data are configured to prevent the use of external media devices (*i.e.*, thumb drives).

g) The site uses a wireless network. If so, we determined if it has a written risk assessment and assessed compliance with the wireless network requirements in Publication 4299.

II. Evaluated IRS processes to identify and address data breaches at Volunteer Program sites, including lost/stolen computers.

A. Determined if sites have written policies and procedures for volunteers to report a suspected data breach to the IRS and if the SPEC function ensures that partners are notified of current guidelines.

B. Assessed the Volunteer Program's controls for ensuring that volunteers report a suspected data breach to the IRS.

1. Interviewed responsible SPEC function officials to assess controls for ensuring that volunteers understand their responsibilities for reporting suspected data breaches and do so.

2. Reviewed reports of stolen/lost computers for FYs 2016, 2017, and 2018 to assess whether reports were received for all known incidents and the reporting adhered to SPEC function procedures.

C. Determined whether the SPEC function analyzes lost or stolen computer theft data for use in enhancing preventative controls in the Volunteer Program.

D. Evaluated the sufficiency and effectiveness of controls for ensuring minimal taxpayer burden and revenue loss related to any breaches.

1. Reviewed reports of lost or stolen computers for FYs 2016, 2017, and 2018 to assess whether the volunteers effectively took the required steps.

a) Reviewed any documentation, such as incident checklists, to evaluate whether the volunteer actions were effective and compliant with guidelines.

b) Evaluated whether volunteers alerted taxpayers regarding breached Personally Identifiable Information. We determined if the volunteers notified the affected taxpayers whose data were stored on the lost or stolen computers in FYs 2016 through 2018.

c) Determined why the SPEC function did not implement a process to add stolen TINs identified from lost or stolen computers and data breaches to the DSL.

III. Determined if the SPEC function implemented controls to ensure the suitability of volunteers.

A. Identified Volunteer Program policies and procedures implemented by the SPEC function and tax partners to ensure that volunteers are suitable to participate and assessed the adequacy of controls to prevent participation when requirements are not met.

B. Assessed the effectiveness of controls for ensuring the suitability of volunteers.

1. Determined if volunteers were meeting the Volunteer Program requirements for participation and if the standards are complete and accurate.

2. Evaluated the effectiveness of the SPEC function's suitability check to identify volunteers who are barred from the Volunteer Program for performing unacceptable practices and who are listed on the Volunteer Registry.

a) Interviewed SPEC function officials to determine policies, procedures, and objectives related to the Volunteer Registry and to ensure its completeness and proper use by sites.

b) Obtained the Volunteer Registry and list of all volunteers for the 2019 Filing Season. We compared the volunteers listed on the Volunteer Registry to the list of 2019 volunteers to identify those who should have been disallowed from participating in the Volunteer Program by matching the last name. For all matches, we manually researched to determine if the person listed on the Volunteer Registry is a volunteer.

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: 1) processes and procedures used to implement controls to safeguard taxpayer data at Volunteer Program sites; 2) processes and procedures to identify and address data breaches at Volunteer Program sites, including lost/stolen computers; and 3) processes and procedures used to ensure the suitability of volunteers. We evaluated these controls by reviewing policies and procedures, interviewing employees and management, and analyzing data.

Appendix II

Major Contributors to This Report

Russell P. Martin, Assistant Inspector General for Audit (Returns Processing and Account Services)
William A. Gray, Director
Levi Dickson, Audit Manager
Stephen Elix, Lead Auditor
Robert Howes, Senior Auditor

Appendix III

Report Distribution List

Deputy Commissioner for Services and Enforcement
Commissioner, Wage and Investment Division
Chief, Communications and Liaison
Director, Customer Assistance, Relationships, and Education, Wage and Investment Division
Director, Stakeholder Liaison Field, Communications and Liaison
Director, Stakeholder Partnerships, Education, and Communication, Wage and Investment Division
Director, Enterprise Audit Management

Appendix IV

Management's Response to the Draft Report

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
ATLANTA, GA 30308

COMMISSIONER
WAGE AND INVESTMENT DIVISION

OCT 18 2019

MEMORANDUM FOR MICHAEL E MCKENNEY
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Kenneth C. Corbin
Commissioner, Wage and Investment Division

SUBJECT: Draft Audit Report – *Actions Are Needed to Improve the Safeguarding of Taxpayer Information at Volunteer Program Sites* (Audit #201840010)

Thank you for the opportunity to review the subject draft report and for acknowledging the important role our Volunteer Program plays in improving taxpayer service and voluntary compliance. The Volunteer Program, which includes the Volunteer Income Tax Assistance (VITA) and Tax Counseling for the Elderly (TCE) programs, offers free tax preparation services to taxpayers in low-to-moderate income ranges and those who may be disabled, limited-English proficient, Native American, or elderly.

The VITA program reached a significant milestone in 2019, marking 50 years of providing free tax preparation assistance to individuals and families. In fiscal year 2019, the program prepared over 3.5 million federal tax returns, in partnership with 82,214 volunteers at 10,921 sites nationwide, resulting in almost $3.5 billion in tax refunds for VITA clients. The returns prepared by the program this year achieved a 99.7 percent electronic filing rate and a 98 percent accuracy rate, the highest accuracy rate ever. As these results show, the VITA and TCE programs positively impact the lives of taxpayers who are served by the programs, as well as those volunteers who donate their time to this worthwhile endeavor.

The integrity of the VITA and TCE programs, and safeguarding taxpayer data, are of paramount importance to the IRS. As such, we continue to work closely with our partners to ensure volunteers comply with our program standards. The partners verify the identity of each of their volunteers by reviewing photo identification. All new volunteers must complete the Volunteer Standards of Conduct (VSC) training and all new and returning volunteers must pass the VSC test before they can volunteer at a site. Individuals who fail to adhere to the VSC are added to a volunteer registry and are barred from returning to the program. Computer and physical security are also key components of protecting taxpayer data. For example, procedures are in place for partners to immediately report stolen IRS computers to law enforcement, and to the IRS

within 48 hours. Reviews are conducted to ensure compliance with site security requirements. These guidelines and procedures are detailed in the Publication 4299, *Privacy, Confidentiality, and Civil Rights - A Public Trust.*

We agree that existing controls can be strengthened to increase the overall security of taxpayer data at the VITA and TCE sites. We also agree that awareness of the Publication 4299 security requirements can be improved. To address this finding, we will increase partner, volunteer, and employee awareness of existing security resources and will modify Publication 4299 to include a security plan template that site coordinators will complete and sign annually. Additionally, we will conduct a Security Symposium prior to the 2020 Filing Season to emphasize the requirements of Publication 4299, the completion of an individualized security plan, and the volunteer registry.

While we will require sites to develop an individualized security plan using the revised Publication 4299, we do not agree with the report's conclusion that the Federal Trade Commission's (FTC's) Safeguards Rule mandates this result from volunteer programs providing free services. We also disagree that the short discussion of the Safeguards Rule in Publication 4600, *Tips for Safeguarding Taxpayer Data*, mandates that VITA and TCE partners and volunteers follow the FTC's Safeguards Rule. The IRS directs Publication 4600 at return preparers, software developers, and other related service providers and not specifically at volunteer sites. Because the Safeguards Rule is an FTC rule, it is ultimately the FTC and not the IRS that has the expertise and authority to determine the scope and application of the Safeguards Rule to entities like VITA and TCE partners and volunteers.

The Volunteer Program has a robust oversight process in place to identify potential security issues at partner locations. We recognize, however, that an increased awareness of our existing controls will ensure continued public confidence in the Volunteer Program. Attached is our response to your recommendations. If you have any questions, please contact me, or a member of your staff may contact Dietra Grant Director, Customer Assistance, Relationships, and Education, Wage and Investment Division, at (470)-639-3443.

Attachment

Attachment

Recommendation

RECOMMENDATION 1
The Commissioner, Wage and Investment Division, should issue guidance to Volunteer Program partners requiring the development of an information security plan for each of their sites. The guidance should detail the elements to be included in this plan and the need to review the plan with volunteers and retain the plan at the site. IRS site review procedures should also be updated to include verification of the information security plan.

CORRECTIVE ACTION
We agree with this recommendation. Publication 4299, *Privacy, Confidentiality, and Civil Rights - A Public Trust*, will be updated to include a security plan template for site coordinators to complete and sign annually. Also, key security topics from Publication 4299 will be highlighted during a partner Security Symposium to increase awareness among internal and external stakeholders.

IMPLEMENTATION DATE
November 15, 2020

RESPONSIBLE OFFICIAL
Director, Stakeholder Partnerships, Education and Communication, Customer Assistance, Relationships and Education, Wage and Investment Division

CORRECTIVE ACTION MONITORING PLAN
We will monitor this corrective action as part of our internal management control system.

Recommendations

The Commissioner, Wage and Investment Division, should:

RECOMMENDATION 2
Require site coordinators to use the security feature included in the tax preparation software to restrict volunteers' access to prepared returns.

CORRECTIVE ACTION
We agree with this recommendation. We will emphasize to site coordinators that they must use the features of tax software that restricts volunteer access to tax returns outside of site operating hours. Also, a question will be added to the Form 6729 Quality Review Job Aid for reviewers to address this issue.

IMPLEMENTATION DATE
November 15, 2020

RESPONSIBLE OFFICIAL
Director, Stakeholder Partnerships, Education and Communication, Customer Assistance, Relationships and Education, Wage and Investment Division

CORRECTIVE ACTION MONITORING PLAN
We will monitor this corrective action as part of our internal management control system.

RECOMMENDATION 3
Develop processes and procedures to confirm site coordinators are aware of security requirements and hold discussions with volunteers at the sites to review these security requirements.

CORRECTIVE ACTION
We agree with this recommendation. The security requirements will be reviewed with site coordinators during the partner Security Symposium. Also, a knowledge check for the Site Coordinator's Training will be implemented to test awareness of procedures.

IMPLEMENTATION DATE
December 15, 2020

RESPONSIBLE OFFICIAL
Director, Stakeholder Partnerships, Education and Communication, Customer Assistance, Relationships and Education, Wage and Investment Division

CORRECTIVE ACTION MONITORING PLAN
We will monitor this corrective action as part of our internal management control system.

RECOMMENDATION 4
Ensure that site reviews include an assessment of compliance with security controls outlined in Publication 4299. This assessment should determine if the site being reviewed uses a wireless computer connection and, if so, that a required risk assessment is completed. The assessment should also include steps to identify and verify proper storage of taxpayer information.

CORRECTIVE ACTION
We agree with this recommendation. The quality review series of forms and job aides will be reviewed to determine what additional questions should be added to address the security controls outlined in Publication 4299 during site reviews.

IMPLEMENTATION DATE
November 15, 2020

RESPONSIBLE OFFICIAL
Director, Stakeholder Partnerships, Education and Communication, Customer Assistance, Relationships and Education, Wage and Investment Division

CORRECTIVE ACTION MONITORING PLAN
We will monitor this corrective action as part of our internal management control system.

RECOMMENDATION 5
Update procedures for partners to validate volunteers' identity using only Government-issued identification prior to participating in the Volunteer Program

CORRECTIVE ACTION
We agree with this recommendation. Procedures will be updated to require validation of volunteers' identity using only government-issued identification prior to participation in the Volunteer Program.

IMPLEMENTATION DATE
December 15, 2020

RESPONSIBLE OFFICIAL
Director, Stakeholder Partnerships, Education and Communication, Customer Assistance, Relationships and Education, Wage and Investment Division

CORRECTIVE ACTION MONITORING PLAN
We will monitor this corrective action as part of our internal management control system.

RECOMMENDATION 6
Reinforce training for SPEC function reviewers and site coordinators on how to report volunteers who are caught violating the Volunteer Standards of Conduct. Site reviewers should confirm an understanding of these processes and procedures with site coordinators as part of the SPEC function's reviews. Training should also address the importance of SPEC function territory managers using the Volunteer Registry to ensure that banned volunteers do not regain entry into the program.

CORRECTIVE ACTION
We agree with this recommendation. Training for Stakeholder Partnerships, Education and Communication function reviewers and site coordinators on how to report volunteers who violate the Volunteer Standards of Conduct will be reinforced. Training will also address using the Volunteer Registry to ensure banned volunteers do not regain entry into the program.

IMPLEMENTATION DATE
March 15, 2020

RESPONSIBLE OFFICIAL
Director, Stakeholder Partnerships, Education and Communication, Customer Assistance, Relationships and Education, Wage and Investment Division

CORRECTIVE ACTION MONITORING PLAN
We will monitor this corrective action as part of our internal management control system.

RECOMMENDATION 7
Develop procedures to evaluate security incidents at Volunteer Program sites to identify affected taxpayers whose information is at risk and forward their TINs to the Return Integrity and Compliance Services function for evaluation and potential inclusion on the DSL. The procedures should include steps to identify taxpayers whose returns were prepared by a volunteer who the SPEC function banned from the Volunteer Program.

CORRECTIVE ACTION
We agree with this recommendation. Procedures for referring Taxpayer Identification Numbers of potentially affected taxpayers to the Dynamic Selection List will be implemented in consultation with the Return Integrity and Compliance Services function.

IMPLEMENTATION DATE
December 15, 2020

RESPONSIBLE OFFICIAL
Director, Stakeholder Partnerships, Education and Communication, Customer Assistance, Relationships and Education, Wage and Investment Division

CORRECTIVE ACTION MONITORING PLAN
We will monitor this corrective action as part of our internal management control system.

RECOMMENDATION 8
Emphasize to all volunteer sites and partners their responsibilities in Publication 4299 to evaluate and report to the IRS all partner-owned and IRS-loaned lost or stolen computers. Site reviewers should confirm the site coordinators' understanding of these procedures during the SPEC function's site reviews. In addition, when lost or stolen computers are reported, ensure that Forms 13747 are prepared and include all information needed to determine the extent to which taxpayer data may be at risk.

CORRECTIVE ACTION
We agree with this recommendation. The issue of reporting lost computers will be addressed during the partner Security Symposium. Questions to confirm understanding of the rules around lost or stolen equipment will be included on a site coordinator knowledge check. Existing guidance will be reviewed to ensure consistency in reporting IRS-and partner-owned equipment that is lost or stolen. All Forms 13747, *Checklist for Lost Equipment* will be reviewed to ensure they are correct and complete.

IMPLEMENTATION DATE
December 15, 2020

RESPONSIBLE OFFICIAL
Director, Stakeholder Partnerships, Education and Communication, Customer Assistance, Relationships and Education, Wage and Investment Division

CORRECTIVE ACTION MONITORING PLAN
We will monitor this corrective action as part of our internal management control system.