TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Analysis of Fiscal Year 2016 Additional Appropriations for Cybersecurity and Identity Theft Prevention Improvements

August 14, 2017

Reference Number: 2017-20-049

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.

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.

ANALYSIS OF FISCAL YEAR 2016 ADDITIONAL APPROPRIATIONS FOR CYBERSECURITY AND IDENTITY THEFT PREVENTION IMPROVEMENTS

Highlights

Final Report issued on August 14, 2017

Highlights of Reference Number: 2017-20-049 to the Internal Revenue Service Deputy Commissioner for Operations Support and Deputy Commissioner for Services and Enforcement.

IMPACT ON TAXPAYERS

Congress appropriated $11.2 billion to the IRS in Fiscal Year 2016, which included $290 million to make measurable improvements in the customer service level of service, to safeguard taxpayer data through enhanced cybersecurity, and to improve the identification and prevention of identity theft and refund fraud.

WHY TIGTA DID THE AUDIT

This audit was initiated to evaluate the process used by the IRS to track and monitor approximately $106.4 million in appropriated funds specifically designated for cybersecurity enhancements and identity theft prevention. Our analysis was performed to address congressional inquiries regarding the IRS's allocation of resources to cybersecurity and identity theft prevention.

WHAT TIGTA FOUND

The IRS adequately tracked and monitored and appropriately spent the additional funding designated for cybersecurity enhancements and identity theft prevention. The IRS allocated approximately $91.8 million of the $290 million in additional funding to safeguard taxpayer data through cybersecurity enhancements. Of the $91.8 million, approximately $71.7 million was obligated in Fiscal Year 2016, with the remaining approximate $20.1 million being obligated in Fiscal Year 2017.

Cybersecurity funding supported network security improvements, more effective monitoring of data traffic, replacement of outdated equipment, and protection of taxpayer data from unauthorized access by identity thieves. TIGTA examined supporting contracts and invoices for 48 requisitions across nine cybersecurity funding categories and determined that the dates, description of work, and dollar amounts were adequately supported and correctly assigned to the appropriated funding account.

In addition, the IRS allocated approximately $14.6 million to identity theft Operations Support to help protect taxpayers by combating identity theft and refund fraud through collaborative efforts with leading tax preparation firms, software developers, payroll and tax financial product processors, and State tax administrators. All of these funds were obligated and spent in Fiscal Year 2016. The funding also supported a web-based authentication application allowing taxpayers to provide proof of identity and increase efficiency for the Taxpayer Protection Program case resolution.

Further, TIGTA determined that the 20 requisitions related to the Actions From the Security Summit and the Get Transcript Relaunch and Analytics obligated for identity theft were adequately supported and included transaction dates, description of work, and dollar amounts and correctly identified the appropriated funding account.

WHAT TIGTA RECOMMENDED

TIGTA made no recommendations in the report. IRS officials reviewed the draft report and agreed with the facts presented.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

August 14, 2017

MEMORANDUM FOR DEPUTY COMMISSIONER FOR OPERATIONS SUPPORT
DEPUTY COMMISSIONER FOR SERVICES AND ENFORCEMENT

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Analysis of Fiscal Year 2016 Additional Appropriations for Cybersecurity and Identity Theft Prevention Improvements (Audit # 201620024)

This report presents the results of our review to evaluate the process used by the Internal Revenue Service (IRS) to track and monitor approximately $106.4 million in appropriated funds specifically designated for cybersecurity enhancements and identity theft prevention. This audit is included in our Fiscal Year 2017 Annual Audit Plan and addresses the major management challenge of Security Over Taxpayer Data and Protection of IRS Resources.

IRS management reviewed the draft report and agreed with the facts presented.

Copies of this report are also being sent to the IRS managers affected by the report information. If you have any questions, please contact me or Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Abbreviations

FY	Fiscal Year
IRS	Internal Revenue Service
PIV	Personal Identity Verification
TIGTA	Treasury Inspector General for Tax Administration

Background

The Internal Revenue Service (IRS) is the largest bureau in the Department of the Treasury and has the primary responsibility for administering the Federal tax system. The IRS's budget request supports the Department of the Treasury's strategic goal of fairly and effectively reforming and modernizing Federal financial management, accounting, and tax systems and the Treasury Priority Goal of increasing self-service and electronic service options for taxpayers.

For Fiscal Year[1] (FY) 2016, Congress provided an appropriation of $11.2 billion to the IRS, which included $290 million to address issues related to customer service, cybersecurity, and identity theft. This additional funding was provided for in the legislation under Section 113 (hereafter referred to as Section 113 funds) of the Administrative Provisions for the IRS[2] and is available until September 30, 2017.[3]

This additional funding was the first significant increase to the IRS budget in six years. In its Spend Plan, the IRS informed Congress as to how the additional funds would be used to increase the telephone level of service, improve the identification and prevention of identity theft, and safeguard taxpayer data through enhanced cybersecurity. This audit focused on the approximately $111.6 million portion of the $290 million appropriation specifically designated for cybersecurity enhancements and identity theft prevention. Specifically, the additional funding was initially allocated in January 2016 for following areas:

Cybersecurity = $95.442 million

- Staffing – $7.0 million
  - This funding is necessary to hire additional staff for remediating critical vulnerabilities, addressing new requirements, and ensuring the protection of critical infrastructure and taxpayer data.
- Unified Access and Segmentation – $4.5 million
  - This funding is for the implementation of a solution to further restrict IRS Local Area Network access and address the lack of segmented network architecture for the IRS Local Area Network.
- Continuous Data Monitoring – $17.2 million

[1] See Appendix IV for a glossary of terms.

[2] Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, Div. E, Title I, § 113, 129 Stat. 2242, 2430-2431 (2015).

[3] The additional $290 million is considered two-year funds, which means the funds can be used one or two years after congressional appropriation.

  - This funding is to support a multiyear program to automate security controls and deficiency management and to standardize risk reporting across Federal agencies.

- Splunk (Database/Analytics Tool in Network Traffic) – $3.0 million
  - This funding is for the purchase of Splunk, which is an industry standard technology that is used to analyze the streams of machine data generated by information technology systems and technology infrastructure in order to improve both insider threat detection and application troubleshooting.
- Cybersecurity Improvement Plan Support – $3.0 million
  - This funding allows the IRS to implement services in response to the goals outlined in the Cybersecurity Strategy and Implementation Plan that was issued by the Office of Management and Budget.
- Aged Server Infrastructure Refresh – $13.0 million
  - This funding is for replacing or retiring outdated technology that supports the development, maintenance, and operations of IRS applications to make processes more secure, reliable, and efficient.
- Security Zone (Cloud Computing) – $20.0 million
  - This funding enables the IRS Information Technology organization to divide content into categories or zones by assigning specific websites to each zone depending on how much trust the content of each site is given.
- Data Loss Prevention – $0.742 million
  - This funding is for the implementation of Safeguarding Personally Identifiable Information Data Extracts subject matter expert support of operations on a 24/7 basis.
- Enterprise Information Technology Security Vulnerability Assessment – $2.0 million
  - This funding supports contractor services and hardware to provide vulnerability assessments via enhanced simulations and exercises.
- Network Getwell Personal Identity Verification (PIV) – $25.0 million
  - This funding is for updating components to the PIV enablement solution. The current PIV enablement in place is a "work-around" for older network devices; the ultimate PIV enablement solution requires updated Cisco software features that will provide improved security. In order to do this, the IRS needs to upgrade its router/switch environment. Funding will replace half of the 57 percent of installed network equipment (or about 28.5 percent of the total inventory) that lacks the necessary software support and needs to be replaced to support PIV

enablement.

Identity Theft Prevention = $16.136 million

- Actions From the Security Summit – $6.136 million
  - This funding helps protect taxpayers by combating identity theft and refund fraud through collaborative efforts with Security Summit participants. Additionally, the funding will support a web-based authentication application allowing taxpayers to provide proof of identity and increasing efficiency for the Taxpayer Protection Program case resolution.
- Get Transcript Relaunch and Analytics – $10.0 million
  - This funding supports the work to enhance the IRS e-Authentication and Get Transcript application relaunch. The IRS Cybersecurity organization is working to develop advanced analytics and fraud detection capabilities. This initiative will produce significant enhancements to metrics, dashboards, and near real-time alerts to warn the IRS of potential suspicious activity.

The IRS is required to operate under a financial plan which shall be based on the most realistic estimates that can be made of programs, staffing, and workload. This financial plan should conform to budget commitments and be followed to the extent approved or as revised by Congress. Any variations to the Spend Plan approved by the IRS Commissioner shall be specified in writing and documented with appropriate support that explains the reasons for and the effect of the variations.

The IRS's budget has four appropriation accounts: 1) Business Systems Modernization; 2) Enforcement; 3) Operations Support; and 4) Taxpayer Services. We concentrated our audit efforts on Operations Support funds which provide support for functions that are essential to the overall operation of the IRS, such as infrastructure and information services.

In addition, appropriation laws set limitations on an agency's ability to reallocate funds between appropriation accounts. Appropriations approved by Congress are intended to provide a mandated framework to support agency activities. Within this framework, agencies may reprogram funds among appropriation accounts and budget activities without requesting statutory authority if the reprogramming will, among other things, augment existing programs, projects, or budget activities by no more than $5 million or 10 percent, whichever is less.

This review was performed with information obtained from the Information Technology organization's Strategy and Planning Financial Management Services office, the Chief Financial Officer, and the Office of Procurement during the period December 2016 through June 2017. Most of the work was performed at these offices located in New Carrollton, Maryland, and Washington, D.C., along with coordinating with other locations for those offices. 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

The Internal Revenue Service's Use of Additional Fiscal Year 2016 Funding for Cybersecurity and Identity Theft Enhancements Was Sufficiently Tracked and Monitored and Appropriately Spent

Overall, the IRS adequately tracked and monitored and appropriately spent the additional funding designated for cybersecurity enhancements and identity theft prevention. From the original Spend Plan established in January 2016, the IRS made slight adjustments to the amounts designated for the various categories when it submitted a revised Spend Plan in May 2016 and when it actually spent the money.

TIGTA reviewed the IRS Spend Plan details for the Section 113 funds and analyzed each line item to determine if the IRS was adequately monitoring and tracking the appropriated funds on the cybersecurity and identity theft items as required and to determine if the expense purpose was consistent and included appropriate authorizing signatures with the account to which funds were charged. Efforts were concentrated on the Operations Support funding as it related to information technology accounts and spending.

Our review of the updated IRS Spend Plan submitted to the House Appropriations Committee on May 24, 2016, showed a reallocation of $20 million from Cybersecurity Security Zone (Cloud Computing), with an additional $16.3 million for Cybersecurity Continuous Data Monitoring and $3.7 million for Operations Support activities within the Identity Theft Prevention Get Transcript Relaunch and Analytics. The IRS is pursuing a different solution to address Security Zone (Cloud Computing) because the project was not approved to proceed to the next phase and the IRS had other critical needs for those funds.

In addition, the original FY 2016 IRS Spend Plan submitted to the House Appropriations Committee on January 27, 2016, showed that, within the identity theft area, the IRS planned to spend $1 million on Operations Support for Actions From the Security Summit. The updated Spend Plan submitted on May 24, 2016, showed a shift of $45,817 from Actions From the Security Summit to the Get Transcript Relaunch and Analytics in addition to the previously mentioned $3.7 million from Cybersecurity Security Zone (Cloud Computing). All other variances between the original January 27, 2016, Spend Plan figures are due to adjustments necessary to more accurately reflect actual expenditures versus the original budget estimates.

Figure 1 represents the approved updated Spend Plan submitted to the House Appropriations Committee on May 24, 2016, which illustrates the changes in the Spend Plan line item obligations.

Figure 1: Updated IRS Spend Plan Submitted to the House Appropriations Committee on May 24, 2016

[money amounts are in thousands of dollars]

Fiscal Year 2016			
Description	**January 2016 Spend Plan**	**May 2016 Updated Spend Plan**	**Change**
Taxpayer Services			
Level of Service - Filing Season 65% / Full Year 47%[1]	$178,422	$178,422	$0
Subtotal, Taxpayer Services	**$178,422**	**$178,422**	**$0**
Cybersecurity[2]			
Staffing	$7,000	$7,000	$0
Unified Access and Segmentation	$4,500	$4,500	$0
Continuous Data Monitoring	$17,200	$33,500	$16,300
Splunk (Database/Analytics Tool in Network Traffic)	$3,000	$3,000	$0
Cybersecurity Improvement Plan Support	$3,000	$3,000	$0
Aged Server Infrastructure Refresh	$13,000	$13,000	$0
Security Zone (Cloud Computing)	$20,000	$0	($20,000)
Data Loss Prevention	$742	$742	$0
Enterprise Information Technology Security Vulnerability Assessment	$2,000	$2,000	$0
Network Getwell Personal Identity Verification	$25,000	$25,000	$0
Subtotal, Cybersecurity	**$95,442**	**$91,742**	**($3,700)**
Identity Theft Prevention[3]			
Actions From the Security Summit	$6,136	$6,136	$0
Get Transcript Relaunch and Analytics	$10,000	$13,700	$3,700
Subtotal, Enforcement (Identity Theft Prevention)	**$16,136**	**$19,836**[4]	**$3,700**
Total, FY 2016 Spend Plan for Section 113 Administrative Provisions	**$290,000**	**$290,000**	**$0**

1 Level of Service improvements include reduction in wait times and improved performance on the Taxpayer Protection Program line.

2 Investments in IRS cybersecurity help to reduce the incidence of identity theft by safeguarding IRS-held taxpayer data from being accessed by identity thieves.

3 The Level of Service and many of the cybersecurity investments are also integral to identity theft prevention by freeing up customer service representatives to answer identity theft questions and by strengthening security controls on IRS systems, improving fraud detection, and providing authentication solutions for taxpayers.

4 TIGTA analysis of Identity Theft Prevention was specific to the Operations Support funding activities as they relate solely to Information Technology functions.

Source: TIGTA comparison of the IRS $290 Million Spend Plan dated January 2016 and the Updated Spend Plan dated May 2016, as reported to Congress.

For the Identity Theft Prevention category of approximately $19.8 million, the IRS designated approximately $14.6 million to Operations Support as it relates solely to Information Technology organization functions, with the remaining balance allocated for Taxpayer Services and Enforcement functions, which we did not include in our review.

Funds for Cybersecurity

The IRS allocated approximately $91.8 million of the $290 million in additional FY 2016 funding it received to improving cybersecurity. Approximately $71.7 (78 percent) of the $91.8 million was obligated and spent in FY 2016, the remaining $20.1 million was obligated and spent in FY 2017.

We examined supporting documentation obtained from the IRS for 48 requisitions across nine cybersecurity funding categories. The supporting documentation included contracts and invoices related to network security improvements, protection of taxpayer data from unauthorized access, and insider threat detection by implementing a system to help analyze information technology system logs. The nine funding categories had amounts totaling approximately $91.8 million. Figure 2 represents the approved updated IRS Spend Plan submitted on May 24, 2016, and reflects the FY 2016 actual amounts and the FY 2017 obligated amounts.

Figure 2: FY 2016 Actual Spent and FY 2017 Obligated Amounts Related to the Updated IRS Spend Plan for Cybersecurity Funding Categories

Cybersecurity Funding Category	Total Actual and Obligated Amounts	FY 2016 Actual Amounts	FY 2017 Obligated Amounts
Staffing	$7,096,796*	$3,848,775	$3,248,021
Unified Access and Segmentation	$4,503,713*	$4,377,367	$126,346
Continuous Data Monitoring	$33,502,228*	$29,161,412	$4,340,816
Splunk (Database/Analytics Tool in Network Traffic)	$3,000,000	$673,423	$2,326,577
Cybersecurity Improvement Plan Support	$3,000,000	$1,322,849	$1,677,151
Aged Server Infrastructure Refresh	$13,000,000	$8,316,964	$4,683,036
Data Loss Prevention	$742,000	$742,000	$0
Enterprise Information Technology Security Vulnerability Assessment	$2,000,000	$2,000,000	$0
Network Getwell Personal Identity Verification	$25,000,000	$21,243,476	$3,756,524
Total	**$91,844,737***	**$71,686,266**	**$20,158,471**

*Source: TIGTA analysis of documentation supporting expenditures for these categories. *The actual money spent on the first three categories in Figure 1 were slightly higher than the updated Spend Plan from May 2016. As a result, the total actual amount spent was $91,844,737 versus $91,742,000 from the May 2016 Spend Plan.*

Based on our analysis of the supporting documentation, we determined the dates, description of work, and dollar amounts were adequately supported and the Section 113 funds were correctly obligated.

Funds for Identity Theft Prevention

The IRS allocated to the Operations Support appropriation account approximately $14.6 million of the additional FY 2016 funding to Identity Theft Prevention to help protect taxpayers by combating identity theft and refund fraud through collaborative efforts with the Security Summit participants. The IRS obligated all funds allocated for Identity Theft Prevention in FY 2016. The funding supported a web-based authentication application allowing taxpayers to provide proof of identity, which increased the efficiency of Taxpayer Protection Program case resolution.

Some of the additional appropriated funds to combat identity theft and refund fraud were used for actions originating from the Security Summit partnership between the IRS, State tax agencies, and the private sector tax industry. This partnership, which marked Calendar Year 2016 as its first year, made progress in implementing several new safeguards, agreeing upon a cybersecurity framework, and taking the initial steps to create a new "early warning" system that will help quickly identify and share identity theft schemes.

To further assist in combating identity theft, in May 2015, the IRS disabled the Get Transcript application, the online service that gave the public electronic access to their tax returns from previous years. The agency discovered that bad actors had stolen personal data from roughly 724,000 taxpayers and used that information to get inside the IRS network. The IRS, with help from the U.S. Digital Service, implemented the Get Transcript Relaunch, which includes a new multifactor authentication framework that meets the standards from the Office of Management and Budget and the National Institute of Standards and Technology.

We examined supporting documentation obtained from the IRS for the Identity Theft Prevention funding category, for funds totaling approximately $14.6 million. We determined that the 20 requisitions reviewed relating to the Actions From the Security Summit and the Get Transcript Relaunch and Analytics obligated for identity theft were adequately supported and included transaction dates, description of work, and dollar amounts.

In the category of Identity Theft Prevention, we reviewed the Information Technology Operations Support appropriation account expenditures of $954,183 to address Actions From the Security Summit. Additionally, we reviewed the Operations Support appropriation account expenditures of $13,643,080 in support of the Get Transcript Relaunch and Analytics. We found that the IRS obligated 100 percent of both funds, $14,597,263 ($954,183 plus $13,643,080), in FY 2016 with nothing to carryover into FY 2017. Figure 3 illustrates the updated Spend Plan amounts as of May 2016 and the actual expenditures for FY 2016.

Figure 3: FY 2016 Actual Spent and FY 2017 Obligated Amounts Related to the Updated IRS Spend Plan for Identity Theft Prevention Funding Categories

Identity Theft Prevention Funding Category	Total Actual and Obligated Amounts	FY 2016 Actual Amounts	FY 2017 Obligated Amounts
Actions From the Security Summit	$954,183	$954,183	$0
Get Transcript Relaunch and Analytics	$13,643,080	$13,643,080	$0
Total	$14,597,263	$14,597,263	$0

Source: TIGTA analysis of documentation supporting expenditures for these categories. The numbers differ from the high-level Updated Spend Plan (May 2016) amounts due to rounding within each spending category and the amounts obligated to Taxpayer Services and Enforcement (see details below).

Security Summit actions include efforts to protect taxpayers from identity theft tax refund fraud, such as improving authentication, communication and taxpayer awareness, financial services, information sharing, strategic threat assessment and response efforts, and tax professionals support.

The Get Transcript Relaunch and Analytics includes a more rigorous e-Authentication process for taxpayers that should significantly increase protection against identity thieves impersonating taxpayers to access tax return information through the IRS Get Transcript online service. The enhanced authentication process should also provide a foundation for additional IRS self-help services in the future.

Our review determined that the IRS has obligated $14,597,263 of the Section 113 funds for identity theft prevention in FY 2016. All of the Section 113 funds were obligated and spent in FY 2016, with a majority of the funding allocated to the Get Transcript Relaunch and Analytics (93 percent).

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to evaluate the process used by the IRS to track and monitor approximately $106.4 million in appropriated funds specifically designated for cybersecurity enhancements and identity theft prevention. To accomplish our objective, we:

I. Determined the methodology used in the FY 2016 Spend Plan for allocating funds to cybersecurity and identity theft prevention enhancements.

- A. Interviewed responsible Chief Financial Officer and business unit financial plan managers regarding processes followed in identifying, tracking, and monitoring marked Section 113 funds' investments.
- B. Obtained and reviewed public law regarding Section 113 funds' expenditures and requirements.
- C. Obtained and reviewed guidance issued by the Department of the Treasury regarding allowable expenses and reporting documentation for Section 113 funds' expenditures.
- D. Identified and reviewed internal controls implemented by the IRS Information Technology organization to track, monitor, and report appropriation expenditures.
- E. Reviewed procedures for monitoring and reporting obligations and expenditures.
- F. Determined if the process for tracking funds is in compliance with Federal financial management reporting guidelines.

II. Determined the effectiveness of the processes and procedures for capturing, tracking, and monitoring Section 113 funds' investments on the Cybersecurity and Identity Theft Prevention Spend Plan.

- A. Interviewed the business unit financial plan managers to determine whether the methodology used to monitor key investments is consistent and adheres to the Chief Financial Officer's policies and procedures.
- B. Evaluated procedures for identifying and charging expenses to the Spend Plan.
- C. Determined if account headings/titles are appropriate for the projects cited in the Spend Plan to allow for proper recording and monitoring.
- D. Compared the use of Business Accounting Codes to the FY 2016 Spend Plan for accuracy.

E. Determined the cut-off cycle for recording, tracking, and monitoring Section 113 funds' expenditures.

III. Determined whether cybersecurity and identity theft prevention expenses are accurately calculated and substantiated by adequate supporting documentation.

A. Compared remaining year-end FY 2016 Spend Plan account balances to the beginning FY 2017 Spend Plan balance.

B. Selected expenditures from all accounts within the Section 113 funds for FY 2016 and reviewed the line items to determine if the expense purpose is consistent with the account to which funds were charged.

C. Reviewed supporting documentation, contracts, and vendor invoices in Step III.B. to determine if the expenditure was properly authorized and accurately recorded.

D. Evaluated compliance with Treasury Spend Plan reporting requirements.

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: Internal Revenue Manual 1.2.10;[1] FY 2016 Financial Management Codes Handbook; IRS 2015 Security Summit Report; Internal Revenue Manual 1.33.4;[2] SOP SS-00X Requisition Reviews and Processing; and the Consolidated Appropriations Act, 2016.[3] We evaluated these controls by conducting interviews and meetings with the Information Technology organization's Cybersecurity office and Identity Theft office employees and Office of Procurement employees. We also reviewed the IRS's retention of invoices related to the Section 113 funds' payments.

[1] Internal Revenue Manual 1.2.10, *Servicewide Policies and Authorities, Policy Statements for Organization, Finance and Management Activities*, dated January 10, 2013.

[2] Internal Revenue Manual 1.33.4, *Strategic Planning, Budgeting and Performance Management*, dated December 16, 2014.

[3] Pub. L. No. 114-113, Div. E, Title I, § 113, 129 Stat. 2242, 2430-2431 (2015).

Appendix II

Major Contributors to This Report

Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services)
Kent Sagara, Director
Joseph F Cooney, Audit Manager
Naomi Butler, Lead Information Technology Specialist
George L. Franklin, Senior Auditor
Suzanne Westcott, Senior Auditor

Appendix III

Report Distribution List

Commissioner
Office of the Commissioner – Attn: Chief of Staff
Chief Financial Officer
Chief Information Officer
Commissioner, Wage and Investment Division
Director, Office of Audit Coordination

Appendix IV

Glossary of Terms

Term	Definition
Appropriation	Statutory authority to incur obligations and make payments out of Treasury funds for specified purposes.
Business Systems Modernization	Appropriation for necessary expenses of the IRS for the capital asset acquisition of information technology systems, including management and related contractual costs of such acquisition and including contractual costs associated with operations as authorized by 5 U.S.C. § 3109.
Chief Financial Officer	The individual primarily responsible for managing the financial risk of an enterprise.
Enforcement	Appropriation for necessary expenses of the IRS to determine and collect owed taxes, to provide legal and litigation support, to conduct criminal investigations, to enforce criminal statutes related to violations of Internal Revenue laws and other financial crimes, to purchase (for police-type use, not to exceed $850) and hire of passenger motor vehicles (31 U.S.C. § 1343(b)), and to provide other services as authorized by 5 U.S.C. § 3109.
Financial Plan	A comprehensive and unified plan of action for carrying out the programs of the IRS during a specified period, expressed in terms of work to be done and staffing and dollars to be devoted thereto. Also called a Spend Plan.
Fiscal Year	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.
Identity Theft	When someone uses an individual's personal information such as name, Social Security Number, or other identifying information without permission to commit fraud or other crimes.
Information Technology	The hardware, software, communication, and other facilities used to input, store, process, transmit, and output data in whatever form.
Level of Service	Calculation of the relative success rate of taxpayers who call seeking assistance from an agent.

Term	Definition
Local Area Network	Communication network that serves several users within a specified geographic area.
Office of Procurement	Provides acquisition services for all business units in the IRS and other bureaus and offices within the Department of the Treasury.
Operations Support	Appropriation for necessary expenses of the IRS to operate and support taxpayer services and tax law enforcement programs, including rent payments; facilities services; printing; postage; physical security; headquarters and other IRS-wide administration activities; research and statistics of income; telecommunications; information technology development, enhancement, operations, maintenance, and security; the hire of passenger motor vehicles (31 U.S.C. § 1343(b)); and other services as authorized by 5 U.S.C. § 3109.
Personal Identity Verification Enablement	An integrated-circuit identification card (PIV Card) that contains identity credentials such as cryptographic keys and biometrics to achieve graduated levels of security, from least secure to most secure, ensuring flexibility in selecting the appropriate level of security for Federal application.
Priority Goal	Target areas where agency leaders want to achieve a near-term performance acceleration through focused senior leadership attention.
Security Summit	The IRS organized a Security Summit meeting on March 19, 2015, in Washington, D.C., with IRS officials; the Chief Executive Officers of the leading tax preparation firms, software developers, and payroll and tax financial product processors; and State tax administrators to discuss common challenges and the ways to leverage collective resources and efforts to protect taxpayers from identity theft refund fraud.
Segmented Network Architecture	Using a firewall, you can separate a network or Local Area Network into multiple components to create segmented network architecture. The firewall blocks data that are not destined for a particular segment and might block all protocol ports except those which that segment specifically requires. Thus, each segment contains filtered and isolated network traffic, which might improve the security and performance of the network. A particular department or a specific group of servers in an organization can use a segment of the corporate Local Area Network, while a bridge, router, or switch separates that segment from the rest of the corporate Local Area Network.

Term	Definition
Taxpayer Protection Program	Responsible for identifying potential identity theft cases that are scored by a set of identity theft models in the Dependent Database or selected through filters in the Return Review Program system; or manually selected by the Integrity and Verification Operation.
Taxpayer Services	Appropriation for necessary expenses of the IRS to provide taxpayer services, including prefiling assistance and education, filing and account services, taxpayer advocacy services, and other services as authorized by 5 U.S.C. § 3109. Taxpayer Services also provides for expenses necessary to implement the health insurance tax credit included in the Trade Act of 2002 (Pub. L. 107-210, Div. A, Title II, §§ 201-203, 116 Stat. 933, 954-972).