HEARING BEFORE THE
COMMITTEE ON THE BUDGET
UNITED STATES SENATE

"Identity Theft"

Testimony of
The Honorable J. Russell George
Treasury Inspector General for Tax Administration

August 26, 2015

Manchester, NH

TESTIMONY
OF
THE HONORABLE J. RUSSELL GEORGE
TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION
before the
COMMITTEE ON THE BUDGET
UNITED STATES SENATE

"Identity Theft"

August 26, 2015

Senator Ayotte, thank you for hosting this hearing and the opportunity to provide testimony on the important subject of identity theft and its impact on the Internal Revenue Service (IRS) and taxpayers.

The Treasury Inspector General for Tax Administration, also known as "TIGTA," is statutorily mandated to provide independent audit and investigative services necessary to improve the economy, efficiency, and effectiveness of the Federal system of tax administration. TIGTA's oversight activities are designed to identify high-risk systemic inefficiencies in IRS operations and to investigate exploited weaknesses in tax administration. TIGTA's role is critical in that we provide the American taxpayer with assurance that the approximately 87,000[1] IRS employees, who collected over $3.1 trillion in tax revenue, processed over 242 million tax returns and other forms, and issued $374 billion in tax refunds[2] during Fiscal Year (FY) 2014, perform their duties in an effective and efficient manner while minimizing the risks of waste, fraud, or abuse.

TIGTA has provided ongoing oversight and testimony on the issue of tax fraud-related identity theft because of the adverse effect on both the victims of this crime and the IRS. Identity theft affects the IRS and tax administration in two ways – fraudulent tax returns and misreporting of income. The IRS has described identity theft as one of its "Dirty Dozen" tax scams and continues to take steps to more effectively detect and prevent the issuance of fraudulent refunds resulting from identity theft tax return filings. Our ongoing audit work shows that while the IRS is making progress in detecting and resolving identity theft issues and providing victim assistance, improvements are still needed.

---

[1] Total IRS staffing as of July 25, 2015. Included in the total are approximately 16,500 seasonal and part-time employees.
[2] IRS, *Management's Discussion & Analysis, Fiscal Year 2014*, page 2.

Since May 2012, my office has issued numerous reports that address the IRS's efforts to detect and prevent the filing of fraudulent tax returns by identity thieves, as well as IRS efforts to assist victims. My comments today will focus on the results of those reports and on our ongoing work to assess the IRS's progress in detecting and resolving identity theft issues related to tax administration.

DETECTION AND PREVENTION OF IDENTITY THEFT

In July 2012,[3] TIGTA issued its first report on our assessment of IRS efforts to detect and prevent fraudulent tax refunds resulting from identity theft. We reported that the impact of identity theft on tax administration is significantly greater than the amount the IRS detects and prevents. For example, our analysis of Tax Year (TY) 2010 tax returns identified approximately 1.5 million undetected tax returns with potentially fraudulent tax refunds totaling in excess of $5.2 billion that had the characteristics of identity theft confirmed by the IRS.

We have continued to perform follow-up reviews evaluating the IRS's efforts to improve detection processes, including its implementing TIGTA recommendations. Most recently,[4] we reported in April 2015 that the IRS continues to make improvements in its identification of identity theft tax returns at the time the returns are processed and before fraudulent tax refunds are released. For example, the IRS reported that in the 2013 Filing Season it detected and prevented approximately $24.3 billion in identity theft refund fraud. These efforts include locking the tax accounts of deceased individuals to prevent others from filing a tax return using their name and Social Security Number (SSN). The IRS locked approximately 26.3 million taxpayer accounts between January 2011 and December 31, 2014. These locks prevent fraudulent tax returns from entering the tax processing system. For Processing Year 2014,[5] the IRS rejected 338,807 e-filed tax returns and stopped 15,915 paper-filed tax returns through the use of these locks as of September 30, 2014.

The IRS also continues to expand the number of filters used to detect identity theft refund fraud at the time tax returns are processed. For example, the IRS increased the number of filters from 80 filters during Processing Year 2013 to 114 filters during Processing Year 2014. The identity theft filters incorporate criteria based on

---

[3] TIGTA, Ref. No. 2012-42-080, *There Are Billions of Dollars in Undetected Tax Refund Fraud Resulting From Identity Theft* (July 2012).
[4] TIGTA, Ref. No. 2015-40-026, *Efforts Are Resulting in the Improved Identification of Fraudulent Tax Returns Involving Identity Theft* (Apr. 2015).
[5] A processing year is the calendar year in which tax returns are processed by the Internal Revenue Service.

characteristics of confirmed identity theft tax returns. Tax returns identified by these filters are held during processing until the IRS can verify the taxpayer's identity. As of September 30, 2014, these filters detected 832,412 tax returns preventing the issuance of approximately $5.5 billion in fraudulent tax refunds.

In addition to the above actions, the IRS has developed and implemented a clustering filter in response to TIGTA's continued identification of large volumes of undetected potentially fraudulent tax returns with tax refunds issued to the same address or deposited into the same bank account. Using this tool, the IRS reported that as of October 9, 2014, it had identified 517,316 tax returns and prevented the issuance of approximately $3.1 billion in fraudulent tax refunds. The IRS has also implemented a systemic restriction to limit the number of deposits (three) to a single bank account beginning with the 2015 Filing Season. TIGTA is evaluating the direct deposit limit as part of our assessment of the IRS's ongoing efforts to detect and prevent identity theft. We expect to issue our report early next fiscal year.[6]

The IRS External Leads Program also assists in the identification and recovery of questionable tax refunds. The program receives leads about questionable tax refunds identified by a variety of partner organizations that include financial institutions, brokerage firms, government and law enforcement agencies, State agencies, tax preparation entities, and others. The program has grown from 10 partner financial institutions and organizations returning $233 million in questionable tax refunds to the IRS in Calendar Year 2010 to 286 returning more than $576 million in Calendar Year 2013.

In August 2014, TIGTA reported[7] that the IRS is not always verifying leads timely; leads are inconsistently tracked in multiple inventory systems; and the inventory systems do not provide key information such as how the lead was resolved, (*i.e.*, refund confirmed as erroneously issued or legitimate).

Notwithstanding improvements in its detection efforts and programs to recover questionable tax refunds that were issued, access to third-party income and withholding information is the key to enabling the IRS to prevent the continued issuance of billions of dollars in fraudulent tax refunds. Most of the third-party income and withholding information is not received by the IRS until well after the tax return filing season begins.

---

[6] TIGTA, Audit No. 201440030, *Effectiveness of Identity Theft Filters in the Return Review Program*, report planned for October 2015.
[7] TIGTA, Ref. No. 2014-40-057, *The External Leads Program Results in the Recovery of Erroneously Issued Tax Refunds, However, Improvements Are Needed to Ensure That Leads Are Timely Verified* (Aug. 2014).

For example, the annual deadline for filing most information returns with the IRS is March 31, yet taxpayers can begin filing their tax returns as early as mid-January each year. For the 2014 Filing Season, the IRS had received approximately 90.8 million tax returns as of March 28, 2014.

Legislation would be needed to accelerate the filing of the information returns. In its Fiscal Year 2015 Revenue Proposal, the IRS again proposed to accelerate the deadline for filing third-party income and withholding information returns and eliminate the extended due date for e-filed information returns. Under this proposal, the information returns would then be required to be filed with the IRS (or the Social Security Administration, in the case of Forms W-2, *Wage and Tax Statement*), by January 31.

The IRS's own analysis estimates that identity thieves were successful in receiving over $5 billion in fraudulent tax refunds in Filing Season 2013. Addressing this issue will require the continued expenditure of resources that could otherwise be used to respond to taxpayer telephone calls, answer correspondence, and resolve discrepancies on tax returns.

The IRS recognizes that new identity theft patterns are constantly evolving and that, as a result, it needs to continuously adapt its detection and prevention processes. For example, identity theft not only affects individuals, but also businesses. The IRS defines business identity theft as creating, using, or attempting to use businesses' identifying information without authority to claim tax benefits. TIGTA reviewed the effectiveness of the IRS's efforts to implement a business return program to detect and prevent identity theft, and found that the IRS has begun to implement processes to detect identity theft on business returns.[8]

However, TIGTA also found that the IRS does not have systemic processes in place to use data it has readily available to proactively identify potential business identity theft at the time tax returns are processed. For example, the IRS maintains a list of suspicious Employer Identification Numbers (EINs)[9] determined to be associated with a fictitious business. Our analysis of business returns filed during Processing Year 2014 identified that 233 tax returns were filed using a known suspicious EIN. In addition, TIGTA determined that processing filters could be developed to identify business tax returns containing certain characteristics that could indicate potential

[8] TIGTA, Audit No. 201440004, *Processes Are Being Established to Detect Business Identity Theft; However, Additional Actions Can Help Improve Detection*, report planned for September 2015.
[9] An EIN is a Federal Tax Identification Number used to identify a taxpayer's business account.

identity theft cases. For example, the IRS has data to proactively identify business tax returns filed using EINs assigned by the IRS to businesses that are not required to file a tax return as well as those that have no recent tax filing history.

Finally, in June 2015, the IRS unveiled its partnership efforts with representatives of tax preparation and software firms, payroll and tax financial product processors and State tax administrators, representing a sweeping new collaborative effort to combat identity theft refund fraud and protect the Nation's taxpayers. Efforts include identifying new steps to validate taxpayer and tax return information at the time of filing; increasing information sharing between industry and governments; and standardized sharing of suspected identity fraud information and analytics from the tax industry to identify fraud schemes and locate indicators of fraud patterns. For the first time, the tax industry will share aggregated analytical information about their filings with the IRS to help identify fraud.

IRS ASSISTANCE TO VICTIMS OF IDENTITY THEFT

Tax-related identity theft adversely affects the ability of taxpayers to file their tax returns and timely receive their tax refunds, often imposing significant financial and emotional hardships. Many taxpayers learn that they are a victim of tax-related identity theft when they attempt to file their electronic tax return and the IRS rejects it because someone else (an identity thief) already filed a return using the same SSN. The IRS advises the taxpayer to submit a paper tax return with an attached Form 14039, *Identity Theft Affidavit*, or police report. TIGTA has reported that the IRS is not always effectively providing assistance to taxpayers who report that they have been victims of identity theft, resulting in an increased burden for those victims.

To provide relief to victims of identity theft, the IRS began issuing Identity Protection Personal Identification Numbers (IP PIN) to eligible taxpayers in Fiscal Year 2011. Use of an IP PIN provides relief to taxpayers because it allows the IRS to process their tax returns without delay and helps prevent the misuse of taxpayers' SSNs on fraudulent tax returns. However, TIGTA has reported that not all eligible individuals are receiving an IP PIN.[10] Specifically, we reported in September 2014 that the IRS did not provide an IP PIN to 532,637 taxpayers who had an identity theft indicator on their tax account indicating that the IRS resolved their case. The IRS also did not provide an IP PIN to 24,628 taxpayers whose Personally Identifiable Information had been lost by

[10] TIGTA, Ref. No. 2014-40-086, *Identity Protection Personal Identification Numbers Are Not Provided to All Eligible Taxpayers* (Sept. 2014).

or stolen from the IRS.

Additionally, In March 2015, we reported that identity theft victims experienced long delays in resolving their tax accounts in Fiscal Year 2013.[11] Our review of a statistically valid sample of 100 identity theft tax accounts resolved by the IRS between October 1, 2012, and September 30, 2013, identified that the IRS took an average of 278 days to resolve the tax accounts. In addition, our review identified that the IRS continues to make errors on the tax accounts of victims of identity theft. For example, of the 100 tax accounts that TIGTA reviewed, the IRS did not correctly resolve 17 accounts (17 percent). Errors result in delayed refunds and require the IRS to reopen cases and take additional actions to resolve the errors. Based on the results of the 100 identity theft tax accounts reviewed, we estimate that of the 267,692 taxpayers whose accounts were resolved during the period October 1, 2012, and September 30, 2013, 25,565 (10 percent) may have been resolved incorrectly, resulting in the issuance of delayed or incorrect refunds. This wastes additional resources needed to resolve the errors and further burdens victims of tax-related identity theft.

As part of the IRS's strategy to reduce taxpayer burden caused by identity theft, it formed the Identity Protection Specialized Unit (IPSU) in October 2008. The IPSU is a dedicated unit that enables victims of identity theft to have their questions answered and issues resolved quickly and effectively. IPSU was originally created with the goal of providing each victim with a dedicated IRS employee to work with each identity theft victim. However, the IRS indicated in November 2014 that budgetary constraints do not allow for a single employee to be assigned to each identity theft victim. The IRS remains committed to continuing to provide victims of identity theft with the centralized IPSU hotline to obtain assistance. The IRS noted that obtaining assistance via contact with the hotline does not depend on the availability of a single IRS representative, who may be unavailable because he or she is performing other casework.

On May 4, 2015, the IRS announced the final phase of its plan to consolidate its identity theft assistance and compliance activities in a new organization called Identity Theft Victim Assistance. The IRS indicated that the new directorate aims to provide consistent treatment to victims of tax-related identity theft. The IRS stated that once the realignment is fully completed, an analysis of all identity theft victim assistance processes, including the IPSU, will be performed. We plan to issue a report in October 2015 of our assessment of whether the IPSU results in a streamlined process to help

[11] TIGTA, Ref. No. 2015-40-024, *Victims of Identity Theft Continue to Experience Delays and Errors in Receiving Refunds* (Mar. 2015).

resolve identity theft cases[12] and plan to review the IRS's implementation of the Identity Theft Victim Assistance directorate next fiscal year.

Finally, to assist victims of identity theft who are working with law enforcement to investigate the theft and use of their personally identifiable information to file a fraudulent tax return, the IRS created its Law Enforcement Assistance Program (LEAP). This program assists law enforcement in obtaining tax return information vital to their efforts in investigating and prosecuting cases of tax-related identity theft. Federal law imposes restrictions on sharing taxpayer information, including information that can be shared with State and local law enforcement. State and local law enforcement officials with evidence of identity theft involving fraudulently filed Federal tax returns must obtain permission from the identity theft victim so the IRS can provide law enforcement with limited tax return information relevant to the identity theft. Through the LEAP, victims of identity theft can provide, and State and local law enforcement can obtain, the required permission.

In November 2014, TIGTA reported that LEAP requests for tax information made through this program were not always timely processed or accurately worked and that the IRS did not always maintain documentation of tax return information provided to the law enforcement officers.[13] We also found that actions are needed to better promote awareness of the LEAP to State and local law enforcement. The IRS has not established an outreach strategy to increase awareness of the LEAP and the benefits the program provides to both the victims of identity theft and law enforcement.

The IRS has also announced it is developing a new process which would give taxpayers online access to view the false tax return that was filed using their SSN. According to the IRS, once the procedures have been finalized, an announcement will be issued to explain the process for receiving a redacted copy of the fraudulent return online to tax-related identity theft victims. As part of TIGTA's ongoing review of the Get Transcript data breach, we have included steps to evaluate the IRS's implementation of this online capability.

Employment-Related Identity Theft

Employment-related identity theft occurs when an identity thief uses a taxpayer's SSN for the purpose of obtaining employment and reporting income. In many cases,

---

[12] TIGTA, Audit No. 201440024, *Improvements Are Needed in the Identity Protection Specialized Unit to Better Assist Victims of Identity Theft*, report planned for October 2015.
[13] TIGTA, Ref. No. 2015-40-003, *Law Enforcement Assistance Program Requests Are Not Always Processed Timely and Accurately* (Nov. 2014).

the unsuspecting taxpayers do not realize they are victims of this type of identity theft until they receive a letter or notice from the IRS. The IRS would issue such a correspondence after it found that a taxpayer's SSN was used by someone else for the purpose of reporting income on an income tax return. In some cases, both the SSN and the taxpayer's name are used; in others, only the SSN is used.

In July 2014, the IRS initiated the *Employment Related Identity Theft Notification Project* to notify a test group of taxpayers that their SSNs have been used by someone other than themselves for the purpose of obtaining employment and reporting income.[14] The pilot initiative was conducted in response to a TIGTA audit recommendation to establish a process to notify a taxpayer when there is evidence that the taxpayer's identity (name and SSN) has been compromised. The IRS mailed approximately 25,000 letters to potential victims of employment-related identity theft whose SSNs had been used on a Form W-2, *Wage on Tax Statement*, accompanying a TY 2013 tax return filed by another individual with an Individual Taxpayer Identification Number (ITIN).[15]

The letters notified the taxpayers that their SSN was used by another person for employment and described steps the taxpayers could take to prevent further misuse of their personal information. The letters also indicated that the IRS could not disclose the identity of the persons using their SSNs. TIGTA is currently evaluating the design, implementation and results of the IRS's notification pilot initiative. We expect to issue our report in February 2016.[16]

OTHER ATTEMPTS TO DEFRAUD TAX ADMINISTRATION ARE INCREASING

The trillions of dollars that flow through the IRS each year and the hundreds of millions of taxpayer data sets it uses and maintains make the IRS an attractive target for criminals who attack the tax administration system for personal gain on a constant basis and in various ways. The scams, and the methods the criminals use to perpetrate them, are constantly changing and require continuous monitoring by the IRS. The IRS annually provides the public with information about what it sees as the "Dirty Dozen" tax scams on its website. These scams range from identity theft to fake charities and

---

[14] IRS, *Employment Related Identity Theft Notification Project – Technical Project Report and Recommendations,* September 2014.
[15] The IRS created the ITIN to provide Taxpayer Identification Numbers, when needed for tax purposes, to individuals who do not have and are not eligible to obtain an SSN.
[16] TIGTA, Audit No. 201540015, *Assistance to Taxpayers Affected by Employment-Related Identity Theft*, report planned for February 2016.

inflated refund claims. The number one "Dirty Dozen" scam affecting taxpayers in 2015 involved aggressive, threatening phone calls from scam artists. In addition to the scams affecting taxpayers, the IRS suffered a data breach when criminals gained unauthorized access to information on tax accounts through the IRS's "Get Transcript" application.

Phone Impersonation Scam

The phone impersonation scam has proven to be so large that it is one of TIGTA's Office of Investigation's top priorities. It is a surprisingly effective and fast way to steal taxpayers' money, and in this fast-paced electronic environment, the money can be gone before the victims realize that they have been scammed. The hundreds of thousands of complaints we have received about this scam makes it the largest, most pervasive impersonation scam in the history of our agency. It has claimed thousands of victims with reported losses totaling over $21.5 million to date.

We first started seeing concentrated reporting of these calls in August 2013. As the number of calls we received continued, we started to specifically track this crime in October 2013. According to the victims, the scam artists made threatening statements and then demanded that the victims immediately put money on prepaid debit cards in order to avoid being arrested. The callers often warned the victims that if they hung up, local police would come to their homes to arrest them. The scammers may also send bogus IRS e-mails to support their scam. Those who fell for the scam withdrew thousands of dollars from their bank accounts and then purchased the prepaid debit cards as instructed by the callers. Once the prepaid debit cards were purchased, the perpetrators instructed the victims to call them back and read them the numbers on the prepaid card. By the time the victims realized they had been scammed, the perpetrators had negotiated the prepaid cards, and the money was gone.

To date, TIGTA has received almost 650,000 reports of these calls. We continue to receive between 9,000 and 12,000 such reports each week. As of August 10, 2015, over 4,200 individuals have been victimized by this scam and they have reported that they have paid a total of over $21.5 million, an average of approximately $5,100 per victim. The highest reported loss by one individual was over $500,000.

The perpetrators do not discriminate; they are calling people everywhere, of all income levels and backgrounds. Based on a review of the complaints we have received, we believe the calls are now being placed from more than one source. This scam is the subject of an ongoing multi-agency investigation. There is much that we are doing to apprehend the perpetrators, but TIGTA is not at liberty to disclose

specifically what is being done as it may impede our ability to successfully bring these criminals to justice. I can tell you that it is a matter of high priority for law enforcement.

However, there is much more that needs to be done, as these examples are part of a broader ring of scam artists operating beyond our borders. This is unfortunately similar to most of the cybercrime we are seeing today – international in nature that utilizes technology (*e.g.*, in the case of the phone fraud scam, the use of Voice over Internet Protocol technology) – and much of it originates from computers outside the United States. The perpetrators use this technology to further deceive their intended victims by, for example, using false telephone numbers that show up on the victim's caller ID systems, making it appear as though the calls are originating from Washington, D.C. or elsewhere in the United States.

Recent IRS Data Breach

On May 26, 2015, the IRS announced that unauthorized access attempts had been made by criminals using taxpayer-specific data to gain access to tax information through the IRS's "Get Transcript" application. As a result of these unauthorized accesses, the IRS deactivated the Get Transcript application on May 21, 2015.

The tax information that can be accessed on the Get Transcript application can include the current and three prior years of tax returns, nine years of tax account information, and wage and income information. To date, the IRS has indicated that unauthorized users were successful[17] in obtaining access to information for over 350,000 taxpayer accounts. However, the actual number of individuals whose personal information was available to criminals accessing these tax accounts is significantly larger, in that these tax accounts include information on all of the individuals claimed on a tax return (e*.g.,* spouses and dependents). IRS analysis also identified over 270,000 additional unauthorized access attempts that failed to clear the authentication processes. The IRS believes that some of this information may have potentially been gathered to file fraudulent tax returns during the upcoming 2016 Filing Season.

According to the IRS, one or more individuals succeeded in clearing an authentication process that required knowledge of information about the taxpayer, including Social Security information, date of birth, tax filing status, and street address. In addition, it appears that these unauthorized users had access to private personal information that allowed them to correctly answer questions which typically only the

[17] A successful access is one in which the unauthorized users successfully answered identity proofing and knowledge-based authentication questions required to gain access to taxpayer account information.

taxpayer would know. This type of information can be purchased from illicit sources or fee-based databases, or obtained from social media sites.

TIGTA's Office of Investigations continues to investigate this incident, coordinating with other Federal law enforcement agencies to determine who is responsible for the intrusion. In addition, the evidence we are gathering is critically important for us to understand the impact on the victims and to document exactly how this happened so it can be prevented in the future.

As part of TIGTA's ongoing review assessing IRS efforts to authenticate individual taxpayers' identities when obtaining services, we determined that the IRS assessed the risk of the Get Transcript application as required. However, the IRS found that the authentication risk associated with Get Transcript was low for both the IRS and taxpayers. The low risk rating resulted in the IRS requiring only single-factor authentication to access the Get Transcript application. While single-factor authentication provides some assurance that an individual attempting to access the online Get Transcript application is actually the taxpayer entitled to such access, the increase in private and public sector data breaches increases the risk that unscrupulous individuals can obtain the information typically required to successfully authenticate someone else's identity. Considering the extent of the information that can be viewed or obtained through the Get Transcript application for the taxpayer as well as the other individuals claimed on a tax return, the IRS should have rated the risk associated with the Get Transcript application as high, which would require a multi-factor authentication in order to grant access.

The IRS is notifying those affected taxpayers by mail regarding the Get Transcript data breach and is placing a protective identity theft marker on their tax accounts to prevent criminals from filing future tax returns using the stolen SSNs. For certain individuals, the IRS will also offer free identity-theft monitoring through an external vendor. TIGTA has a review ongoing to evaluate IRS assistance provided to victims of the Get Transcript data breach. We plan to issue our interim report on the accounts that IRS initially identified in January 2016.[18]

The proliferation of data breaches reported in recent years and the types of information available on the Internet has resulted in a degradation of controls used to authenticate individuals accessing personal data in some systems. Providing taxpayers more avenues to obtain answers to their tax questions or to access their own tax

[18] TIGTA, Audit No. 201540027, *Evaluation of Assistance Provided to Victims of the Get Transcript Data Breach*, report planned for January 2016.

records online also creates greater risk to an organization and provides more opportunities for exploitation by hackers and other fraudsters. In its most recent Strategic Plan,[19] the IRS acknowledged that the current technology environment has raised taxpayers' expectations for online customer service interactions. However, the risk for this type of unauthorized access to tax accounts will continue to grow as the IRS focuses its efforts on delivering taxpayers self-assisted interactive online tools.

We at TIGTA remain concerned about the ever-increasing attempts to defraud taxpayers through identity theft and other scams. Because of the importance of these issues, we plan to provide continuing audit coverage of the IRS's efforts to prevent tax-related identity theft and will continue to investigate any instances of attempts to corrupt or otherwise interfere with the Nation's system of tax administration.

Senator Ayotte, thank you for the opportunity to update you on our work on this critical tax administration issue and to share my views.

[19] *Internal Revenue Service Strategic Plan – FY 2014-2017* (IRS Publication 3744), pgs. 6-7 (June 2014).

J. Russell George

Treasury Inspector General for Tax Administration

Following his nomination by President George W. Bush, the United States Senate confirmed J. Russell George in November 2004, as the Treasury Inspector General for Tax Administration. Prior to assuming this role, Mr. George served as the Inspector General of the Corporation for National and Community Service, having been nominated to that position by President Bush and confirmed by the Senate in 2002.

A native of New York City, where he attended public schools, including Brooklyn Technical High School, Mr. George received his Bachelor of Arts degree from Howard University in Washington, DC, and his Doctorate of Jurisprudence from Harvard University's School of Law in Cambridge, MA. After receiving his law degree, he returned to New York and served as a prosecutor in the Queens County District Attorney's Office.

Following his work as a prosecutor, Mr. George joined the Counsel's Office in the White House Office of Management and Budget where he was Assistant General Counsel. In that capacity, he provided legal guidance on issues concerning presidential and executive branch authority. He was next invited to join the White House Staff as the Associate Director for Policy in the Office of National Service. It was there that he implemented the legislation establishing the Commission for National and Community Service, the precursor to the Corporation for National and Community Service. He then returned to New York and practiced law at Kramer, Levin, Naftalis, Nessen, Kamin & Frankel.

In 1995, Mr. George returned to Washington and joined the staff of the Committee on Government Reform and Oversight, where he served as the Staff Director and Chief Counsel of the Government Management, Information and Technology subcommittee (later renamed the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations), chaired by Representative Stephen Horn. There he directed a staff that conducted over 200 hearings on legislative and oversight issues pertaining to Federal Government management practices, including procurement policies, the disposition of government-controlled information, the performance of chief financial officers and inspectors general, and the Government's use of technology. He continued in that position until his appointment by President Bush in 2002.

In addition to his duties as the Inspector General for Tax Administration, Mr. George serves as a member of the Recovery Accountability and Transparency Board, a non-partisan, non-political agency created by the American Recovery and Reinvestment Act of 2009 to provide unprecedented transparency and to detect and prevent fraud, waste, and mismanagement of Recovery funds. There, he serves as chairman of the Recovery.gov committee, which oversees the dissemination of accurate and timely data about Recovery funds.

Mr. George also serves as a member of the Integrity Committee of the Council of Inspectors General for Integrity and Efficiency (CIGIE). CIGIE is an independent entity within the executive branch statutorily established by the Inspector General Act, as amended, to address integrity, economy, and effectiveness issues that transcend individual Government agencies; and increase the professionalism and effectiveness of personnel by developing policies, standards, and approaches to aid in the establishment of a well-trained and highly skilled workforce in the offices of the Inspectors General. The CIGIE Integrity Committee serves as an independent review and investigative mechanism for allegations of wrongdoing brought against Inspectors General.