HEARING BEFORE THE
COMMITTEE ON SMALL BUSINESS
U.S. HOUSE OF REPRESENTATIVES

"Scam Spotting: Can the IRS Effectively Protect Small Business Information?"

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

April 6, 2017

Washington, D.C.

TESTIMONY
OF
THE HONORABLE J. RUSSELL GEORGE
TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION
before the
COMMITTEE ON SMALL BUSINESS
U.S. HOUSE OF REPRESENTATIVES

"Scam Spotting: Can the IRS Effectively Protect Small Business Information?"
April 6, 2017

Chairman Chabot, Ranking Member Velazquez, and Members of the Committee, thank you for the opportunity to testify on identity theft and its impact on the Internal Revenue Service (IRS) and taxpayers.

The Treasury Inspector General for Tax Administration (TIGTA) was created by Congress in 1998 and is mandated to ensure integrity in America's tax system. It provides independent audit and investigative services to improve the economy, efficiency, and effectiveness of IRS operations. TIGTA's oversight activities are designed to identify high-risk systemic inefficiencies in IRS operations and to investigate exploited weaknesses in tax administration. TIGTA plays the key role of ensuring that the approximately 83,000 IRS employees[1] who collected more than $3.3 trillion in tax revenue, processed more than 244 million tax returns, and issued more than $400 billion in tax refunds during Fiscal Year (FY) 2016,[2] have done so in an effective and efficient manner while minimizing the risk of waste, fraud, and 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 continues to remain on the IRS's list of "Dirty Dozen" top tax scams. To address the scam, the IRS 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 the IRS is making progress in detecting and resolving identity-theft issues and providing victim assistance. However, our work also shows that improvements are still needed.

[1] Total IRS staffing as of January 7, 2017. Included in the total are approximately 16,200 seasonal and part-time employees.
[2] IRS, *Management's Discussion & Analysis, Fiscal Year 2016*.

Since May 2012, my office has issued numerous reports that address the IRS's efforts to detect and prevent the filing of fraudulent individual and business 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

Identity-theft tax refund fraud occurs when an individual uses another person's name and Taxpayer Identification Number[3] to file a fraudulent tax return. Unscrupulous individuals steal identities for use in submitting tax returns with false income and withholding documents to the IRS for the sole purpose of receiving a fraudulent tax refund. Identity-theft tax refund fraud affects both individuals and businesses.

In July 2012,[4] 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 that the IRS detects and prevents. For example, our analysis of Tax Year (TY) 2010 tax returns identified approximately 1.5 million undetected individual tax returns that had the characteristics of identity theft confirmed by the IRS, with potentially fraudulent tax refunds totaling in excess of $5.2 billion.

We have continued to perform follow-up reviews evaluating the IRS's efforts to improve detection processes, including its implementation of TIGTA recommendations. Most recently, we reported in February 2017[5] that IRS efforts are resulting in improved detection of identity theft individual tax returns at the time returns are processed and before fraudulent tax refunds are released. For example, the IRS reported in its October 2016 Identity Theft Taxonomy Analysis that for TY 2014 it had detected and prevented approximately $12 billion in identity theft refund fraud.

For the 2017 Filing Season, the IRS is using 197 identity-theft filters to identify potentially fraudulent individual tax returns and prevent the issuance of fraudulent tax

---

[3] A nine-digit number assigned to taxpayers for identification purposes. Depending upon the taxpayer, the number can be an Employer Identification Number, a Social Security Number (SSN), or an Individual Taxpayer Identification Number.

[4]. TIGTA, Ref. No. 2012-42-080, *There Are Billions of Dollars in Undetected Tax Refund Fraud Resulting From Identity Theft* (July 2012).

[5] TIGTA, Ref. No. 2017-40-017, *Efforts Continue to Result in Improved Identification of Fraudulent Tax Returns Involving Identity Theft; However, Accuracy of Measures Needs Improvements* (Feb. 2017).

refunds. These filters incorporate criteria based on characteristics of confirmed identity-theft tax returns, including characteristics such as amounts claimed for income and withholding, filing requirements, prisoner status, taxpayer age, and filing history. Tax returns identified by these filters are held during processing until the IRS can verify the taxpayer's identity. The IRS attempts to contact the individual who filed the tax return and, if the individual's identity cannot be confirmed, the IRS removes the tax return from processing. This prevents the issuance of many fraudulent tax refunds. As of March 2, 2017, the IRS reported that it had identified and confirmed 14,068 fraudulent tax returns and prevented the issuance of $91.9 million in fraudulent tax refunds as a result of the identity-theft filters.

Also, beginning with the 2017 Filing Season, the IRS has access to third-party income and withholding information to compare against tax returns during processing. In December 2015, Congress passed legislation to address TIGTA's ongoing concern about limitations in the IRS's ability to prevent the continued issuance of billions of dollars in fraudulent tax refunds.[6] We had previously reported that the IRS did not have timely access to third-party income and withholding information needed to make substantial improvements in its fraud detection efforts. Beginning in 2017, the enacted legislation now requires the annual filing of income and withholding information by January 31. Access to this information at the beginning of the filing season is the single most important tool to detect and prevent tax fraud-related identity theft. TIGTA will be reviewing the IRS's use of the income and withholding information returns as part of its FY 2017 assessment of the IRS's efforts to detect and prevent identity theft.

To prevent fraudulent tax returns from entering the tax processing system, the IRS continues to expand its processes to reject e-filed tax returns and prevent paper tax returns from posting. For example, as of March 13, 2017, the IRS locked approximately 33.2 million taxpayer accounts of deceased individuals. The locking of a tax account results in the rejection of an e-filed tax return and the prevention of a paper-filed tax return from posting to the Master File if the Social Security Number (SSN) associated with a locked tax account is used to file a tax return. According to the IRS, as of February 28, 2017, it had rejected approximately 10,954 fraudulent e-filed tax returns, and, as of March 16, 2017, it had stopped 2,317 paper-filed tax returns from posting to the Master File.

In addition, in response to concerns raised by TIGTA regarding multiple refunds going to the same address or bank account, the IRS now uses a clustering filter tool to group tax returns based on characteristics that include the address, zip code, and bank

---

[6] Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, Div. Q, § 201 (2015).

routing numbers. For the tax returns identified, the IRS uses criteria in an attempt to ensure that legitimate taxpayers are not included. Tax returns identified are withheld from processing until the IRS can verify the taxpayer's identity. As of March 2, 2017, the IRS reports that, using this tool, it has identified 72,622 tax returns and prevented the issuance of approximately $334.6 million in fraudulent tax refunds.

Beginning with the 2015 Filing Season, the IRS also implemented a systemic restriction to limit the number of deposits (three) to a single bank account. The IRS will convert the fourth and subsequent direct deposit refund requests to paper checks and send them to the taxpayers' addresses of record. In January 2017,[7] we reported that our analysis of direct deposit requests made as of May 5, 2016, identified 5,605 direct deposit attempts totaling approximately $9.2 million that did not convert to paper checks as required. We are evaluating IRS programming changes implemented to address the errors that we identified as part of our ongoing 2017 Filing Season review.

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. These evolving identity-theft patterns affect not only individuals, but also businesses. The IRS defines business identity theft as creating, using, or attempting to use a business's identifying information without authority, in order to claim tax benefits. For example, in order to obtain a fraudulent refund, an identity thief files a business tax return (*e.g.*, Form 1120, *U.S. Corporation Income Tax Return*, Form 720, *Quarterly Federal Excise Tax Return,* or Form 941, *Employer's QUARTERLY Federal Tax Return*) using the Employer Identification Number (EIN)[8] of an active or inactive business without the permission or knowledge of the EIN's owner. As another example, an identity thief applies for and obtains an EIN using the name and SSN of another individual as the responsible party (*i.e.*, fraudulently obtained EIN), without that individual's approval or knowledge, and uses it to create fictitious Forms W-2, *Wage and Income Statement* and bogus Forms 1040, *U.S. Individual Income Tax Return*, which the thief then files to claim a fraudulent refund.

In September 2015, we reported that the IRS recognized the growing threat of business related identity theft and, in response, was implementing processes to detect

---

[7] TIGTA, Ref. No. 2017-40-014, *Results of the 2016 Filing Season* (January 2017).

[8] An EIN is a Federal Tax Identification Number used to identify a taxpayer's business account. The EIN is a nine-digit number (in the format of xx-xxxxxxx) assigned by the IRS and used by employers, sole proprietors, corporations, partnerships, nonprofit associations, trusts and estates, government agencies, certain individuals, and other types of businesses.

identity theft on business returns at the time tax returns are processed.[9] These efforts included conducting a *Business Identity Theft Project* to detect potential business identity theft relating to the filing of Forms 1120 reporting overpayments and claiming refundable credits.

However, TIGTA also found that the IRS is not using data it has readily available to proactively identify potential business identity theft. For example, the IRS maintains a cumulative list of suspicious EINs that it has determined to be associated with fictitious businesses. As of March 24, 2015 the list included 6,176 suspicious EINs. Our analysis of business returns filed during Processing Year[10] 2014 identified 233 tax returns that were filed using a known suspicious EIN. Of these, 97 businesses claimed refunds totaling over $2.5 million. In response to TIGTA's recommendations, the IRS is expanding its filters to identify business identity theft. For the 2017 Filing Season, the IRS is using 25 identity theft filters to identify potentially fraudulent business tax returns and prevent the issuance of fraudulent tax refunds. TIGTA is planning a follow-up audit to assess the IRS's efforts to expand on its processes and procedures to detect business identity theft.

To further protect businesses that file employment tax returns, the Consolidated Appropriations Act of 2014[11] requires the IRS to issue a notice to these employers to confirm any address change. The intent of the notice is to make employers aware of address changes so they can contact the IRS if they did not authorize the address change. Address changes can occur for a variety of reasons, including the filing of a fraudulent employment tax return with a new address by an identity thief. The IRS is required to send a notice to both the employer's former and new address. The IRS implemented the required notice program in January 2015 and reports that for FY 2017 over 2 million sets of notices have been issued as of March 25, 2017. TIGTA is currently conducting a review to evaluate the effectiveness of this dual notification process.[12]

While the IRS's identification and detection strategies have led to many notable improvements, it recognizes the need to continue to explore other initiatives that would assist with its overall detection and prevention efforts. These initiatives include a collaborative effort among IRS officials, representatives from leading tax preparation

---

[9] TIGTA Ref. No. 2015-40-082, *Processes Are Being Established to Detect Business Identity Theft; However, Additional Actions Can Help Improve Detection* (Sept. 2015).
[10] The calendar year in which the tax return or document is processed by the IRS.
[11] Consolidated Appropriations Act, 2014, Pub. L. No. 113-76, Div. E, § 106 (2014).
[12] TIGTA Audit 201640019, *Professional Employer Organization Certification Process*, report scheduled for August 2017.

firms, software developers, payroll and tax financial product processors, and representatives from the State Departments of Revenue to discuss common challenges and ways to leverage collective resources and efforts for identity theft detection and prevention. Additionally, the IRS obtains leads about potential identify theft tax returns from State tax agencies via its *State Suspicious Filer Exchange Initiative*, and is conducting a pilot initiative with select payroll providers to test the feasibility of using a verification code to authenticate Form W-2 data at the time tax returns are processed.

IRS ASSISTANCE TO VICTIMS OF IDENTITY THEFT

Tax-related identity theft adversely affects the ability of innocent 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) has already filed a return using the same SSN. Individuals can also learn that they are victims of employment-related identity theft if they receive a notification from the IRS of an income discrepancy between the amounts reported on their tax returns and the amount employers reported to the IRS. This can occur when an innocent taxpayer's stolen identity is used by someone else to gain employment. It can cause a significant burden, due to the incorrect computation of taxes and Social Security benefits based on income that does not belong to the taxpayer.

TIGTA has reported that the IRS does not always effectively provide assistance to taxpayers who report that they have been victims of identity theft, resulting in an increased burden for those victims. Specifically, TIGTA reviews have identified long delays in case resolution and account errors, and have found that not all tax-related identity-theft victims receive Identity Protection Personal Identification Numbers (IP PIN).[13] For example, in March 2015,[14] we reported that victims continue to experience long delays while waiting for the IRS to resolve their cases and issue their refunds. 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, revealed that the IRS took an average of 278 days to resolve the tax accounts. Our report also found that IRS employees did not correctly resolve 17 of the 100 tax accounts. We reported that an estimated 25,565 (10 percent) of the 267,692 taxpayers whose

---

[13] An IP PIN is a six-digit number assigned to taxpayers that allows their tax returns/refunds to be processed without delay and helps prevent the misuse of their SSNs to file fraudulent Federal income tax returns.

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

accounts were resolved may have been resolved incorrectly, resulting in a delayed issuance of refunds to some victims or in some victims receiving an incorrect refund amount.

In July 2015, the IRS created the Identity Theft Victim Assistance (IDTVA) Directorate to combine the skills of employees working tax-related identity-theft cases in multiple functions into one directorate. The goal is to improve the taxpayer's experience when working with the IRS to resolve his or her tax-related identity-theft case. Approximately 1,300 employees work in the IDTVA Directorate to resolve taxpayer-initiated identity-theft cases.[15] TIGTA's current review[16] of cases closed from August 1, 2015, through May 25, 2016, identified improvements in case closure timeframes and a reduction in case closing errors in comparison to our prior audit completed before the IDTVA Directorate was created. The IRS's efforts to centralize operations under a unified leadership, along with its enhanced procedures and processes, have contributed to the improvements identified since our prior audit. We plan to issue our final report in May 2017.

To provide relief to tax-related identity-theft victims, the IRS began issuing IP PINs to eligible taxpayers in FY 2011. For Processing Year 2016, the IRS issued more than 2.7 million IP PINs to taxpayers for use in filing their tax returns. In March 2017, TIGTA reported that some improvements are needed.[17] Specifically, TIGTA found that taxpayer accounts were not always consistently updated to ensure that IP PINs were generated for taxpayers as required. For example, the IRS did not generate IP PINs for more than 2 million taxpayers for whom the IRS resolved an identity-theft case by confirming that the taxpayer was a victim. This results from inconsistent processes and procedures when closing resolved identity-theft cases. Without the required marker on their account to generate an IP PIN, these taxpayers will experience delays when tax returns are subsequently filed.

In November 2016, TIGTA reported that additional actions can be taken to improve the accuracy and timeliness of processing tax return requests from victims of

---

[15] A taxpayer-initiated identity theft case is created when taxpayers contact the IRS to report that after filing their tax return they received a notice indicating the return was rejected because someone (an identity thief) already filed a return using the same SSN and name.

[16] TIGTA, Audit No. 201640015, *Identity Theft Victim Assistance Directorate*, report scheduled for April 2017.

[17] TIGTA, Ref. No. 2017-40-026, *Inconsistent Processes and Procedures Result in Many Victims of Identity Theft Not Receiving Identity Protection Personal Identification Numbers* (Mar. 2017).

tax-related identity theft.[18] In 2015, the IRS changed its policy to allow identity-theft victims to receive, upon request, redacted copies of fraudulent tax returns filed using their names and SSNs. To process taxpayer requests, the IRS established a new program called the Fraudulent Return Request Program. According to the IRS, it has received, as of December 31, 2016, more than 7,200 requests for copies of fraudulent returns since the program's inception in November 2015.

While the IRS took prompt action to establish this program, as of March 11, 2016, TIGTA's review of a statistically valid sample of 130 taxpayer requests, from a population of 1,962 taxpayer requests, identified 33 taxpayer requests with one or more processing errors. Based on the results of this sample, TIGTA projects that 498 taxpayers' requests could contain processing errors. The errors identified by TIGTA included not timely processing the request, not providing a copy of the fraudulent tax return, and not properly redacting all required information from the return, such as taxpayer names, street numbers, and telephone numbers.

In August 2016, we reported that during the period February 2011 to December 2015, the IRS identified almost 1.1 million taxpayers who were victims of employment-related identity theft, but who were not notified.[19] During this audit, the IRS announced it would begin notifying victims of employment identity theft starting in January 2017. The notification letter describes steps the taxpayers could take to prevent further misuse of their personal information, including reviewing their earnings with the Social Security Administration to ensure that their records are correct. TIGTA is currently conducting a review to assess IRS actions to notify victims, and we plan to issue our draft report in November 2017.[20]

We have an ongoing audit that is evaluating the IRS's processes to identify and mark victims' tax accounts and to notify the Social Security Administration to ensure that individuals' Social Security benefits are not affected by the misuse of their identities by imposters to gain employment.[21] TIGTA found that IRS processes are not sufficient to identify all employment identity-theft victims. In addition, IRS processes do not identify employment identity theft when processing paper tax returns, nor does the

---

[18] TIGTA, Ref. No. 2017-40-011, *Actions Can Be Taken to Improve Processes of a Newly Developed Program That Enables Victims of Identity Theft to Request Copies of Fraudulent Tax Returns* (Nov. 2016).
[19] TIGTA, Ref. No. 2016-40-065, *Processes Are Not Sufficient to Assist Victims of Employment-Related Identity Theft* (Aug. 2016).
[20] TIGTA, Audit No. 201740033, *Notification Letters to Victims of Employment Identity Theft*.
[21] TIGTA, Audit No. 201640028, *Employment Related Identity Theft – Returns Processing*, report scheduled for April 2017.

IRS have a process to notify the Social Security Administration of employment identity theft when both the victim's name and SSN are used by imposters to gain employment. TIGTA expects to issue its report in May 2017.

TELEPHONE IMPERSONATION SCAM

Since the fall of 2013, a significant amount of our Office of Investigations' workload has consisted of investigating a telephone impersonation scam in which more than 1.9 million intended victims have received unsolicited telephone calls from individuals falsely claiming to be IRS or Department of the Treasury employees. The callers demand money under the pretense that the victim owes unpaid taxes. To date, over 10,300 victims have purportedly paid more than $55 million to these criminals.

The telephone impersonation scam continues to be one of TIGTA's top priorities; it has also landed at the top of the IRS's "Dirty Dozen" tax scams. The numbers of complaints we have received about this scam have cemented its status as the largest, most pervasive impersonation scam in the history of our agency. It has claimed victims in every State.

Here is how the scam works: the intended victim receives an unsolicited telephone call from a live person or from an automated call dialer. The caller, using a fake name and sometimes a fictitious IRS employee badge number, claims to be an IRS or Treasury employee. The scammers use Voice over Internet Protocol technology to hide their tracks and create false telephone numbers that show up on the victim's caller ID system. For example, the scammers may make it appear as though the calls are originating from Washington, D.C., or elsewhere in the United States, when in fact they may be originating from a call center located in India.

The callers may even know the last four digits of the victim's SSN or other personal information about the victim. The caller claims that the intended victim owes the IRS taxes and that, if those taxes are not paid immediately, the victim will be arrested or charged in a lawsuit. Other threats for non-payment include the loss of a driver's license, deportation, or loss of a business license. They often leave "urgent" messages to return telephone calls and they often call the victim multiple times.

According to the victims we have interviewed, these scammers then demanded that the victims immediately pay the money using Apple iTunes® gift cards, Target gift cards, prepaid debit cards, wire transfers, Western Union payments or MoneyGram® payments in order to avoid being immediately arrested. They are typically warned that if they hang up, local police will come to their homes to arrest them immediately. Sometimes the scammers also send bogus IRS e-mails to support their claims that

they work for the IRS. By the time the victims realize that they have been scammed, the funds are long gone.

TIGTA has made several arrests in connection with this scam and has numerous investigations underway. In July 2015, in one of the largest prosecutions on this scam that we have had to date, an individual plead guilty to organizing an impersonation scam ring. He was sentenced to over 14 years of incarceration and ordered to forfeit $1 million. In October of 2016, after an extensive three-year investigation, TIGTA, the Department of Justice and the Department of Homeland Security announced the indictment of 56 individuals and five call centers located in India. Although the investigations and prosecutions have reduced the number of scam calls being placed by over 90 percent, we are still receiving reports that between 5,000 and 6,000 people are receiving calls each week.

In addition to the criminal prosecutions, to thwart scammers using robo-dialers, we have created and instituted an "Advise and Disrupt" strategy. The strategy involves cataloguing the telephone numbers that have been reported by intended victims. We then use our own automated call dialers to make calls to those telephone numbers to advise the scammers that their activity is criminal and to cease and desist their activity. Utilizing this technique, we have placed more than 142,000 automated calls back to the scammers. We are also working with the telephone companies to have the scammers' telephone numbers shut down as soon as possible. Of the 1,160 telephone numbers that have been reported by victims, we have successfully shut down 94 percent of them, some of them within one week of the number's being reported to us.

TIGTA is also publishing those scam related telephone numbers on the Internet. This provides intended victims an additional tool to help them determine if the call is part of a scam. All they have to do is type the telephone number in any search engine, and the response will indicate whether the telephone number has been identified as part of the impersonation scam. These efforts are producing results: our data show it now takes hundreds of calls to defraud one victim, whereas in the beginning of the scam it took only a double digit number of attempts.

TIGTA is also engaged in public outreach efforts to educate taxpayers about the scam. These efforts include publishing press releases, granting television interviews, issuing public service announcements, and providing testimony to Congress. The criminals view this scam as they do many others; it is a crime of opportunity. Unfortunately, while we plan on arresting and prosecuting more individuals, the scam will not stop until people stop paying the scammers money. Our best chance at defeating this crime is to educate people so they do not become victims in the first place. Every innocent taxpayer we protect from this crime is a victory.

We at TIGTA take seriously our mandate to provide independent oversight of the IRS in its administration of our Nation's tax system. As such, we plan to provide continuing audit coverage of the IRS's efforts to identify and detect identity theft and provide assistance to victims.

Chairman Chabot, Ranking Member Velazquez, and Members of the Committee, thank you for the opportunity to share my views.

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 and 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.

Mr. George also served 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 to 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.