JOINT HEARING BEFORE THE
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
SUBCOMMITTEE ON HEALTH CARE, BENEFITS
AND ADMINISTRATIVE RULES, AND
SUBCOMMITTEE ON GOVERNMENT OPERATIONS,
U.S. HOUSE OF REPRESENTATIVES

"Ongoing Management Challenges at IRS"

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

October 25, 2017

Washington, D.C.

TESTIMONY
OF
THE HONORABLE J. RUSSELL GEORGE
TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION
before the
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
SUBCOMMITTEE ON HEALTH CARE, BENEFITS
AND ADMINISTRATIVE RULES, AND
SUBCOMMITTEE ON GOVERNMENT OPERATIONS,
U.S. HOUSE OF REPRESENTATIVES

"Ongoing Management Challenges at IRS"
October 25, 2017

Chairman Jordan, Chairman Meadows, Ranking Member Krishnamoorthi, Ranking Member Connolly, and Members of the Subcommittees, thank you for the opportunity to testify on some of the ongoing challenges facing the Internal Revenue Service (IRS). Specifically, my testimony today will focus on the results of our recent audit work related to the IRS's process of rehiring former employees, the challenges of information security and modernizing information technology infrastructure at the IRS, and the IRS's use of critical pay authority to hire employees.

The Treasury Inspector General for Tax Administration (TIGTA) was created by Congress in 1998 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 85,000 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[2] (FY) 2016,[3] have done so in an effective and efficient manner while minimizing the risk of waste, fraud, and abuse.

[1] In FY 2016, the IRS employed, on average, approximately 85,000 people, including more than 16,000 temporary and seasonal staff.
[2] The Federal Government's fiscal year begins on October 1 and ends on September 30.
[3] IRS, *Management's Discussion & Analysis, Fiscal Year 2016*.

FOLLOW-UP REVIEW OF THE IRS'S PROCESS TO REHIRE FORMER EMPLOYEES

In December 2014, TIGTA reported that, although the IRS appropriately applied Office of Personnel Management (OPM) suitability standards, 824 (11.5 percent) of 7,168 former IRS employees rehired between January 1, 2010, and September 30, 2013, had prior substantiated conduct or performance issues.[4] IRS officials stated that prior conduct and performance issues did not play a significant role in deciding which candidates were best qualified for hiring, and TIGTA found nothing in the IRS hiring process beyond the suitability standards where prior conduct and performance issues were being considered. In addition, we reported that the IRS had prior IRS employment information that could help inform its decisions on hiring. However, the IRS was concerned that it might violate existing Federal regulations if it fully considered prior conduct and performance issues.

As a result, we recommended that the IRS Human Capital Officer work with General Legal Services and the OPM to determine whether, and during what part of the hiring process, the IRS could fully consider prior conduct and performance issues. The IRS agreed with this recommendation. In its response, the IRS stated that a review of conduct and performance issues could be accomplished earlier in the process; however, the Department of the Treasury, the OPM, and the IRS believed that it was not feasible to move the review of these issues to earlier in the hiring process. They concluded that this action would greatly increase the cost of hiring, likely increase cycle time beyond the Presidential mandate of 80 calendar days, require additional resources, and not likely yield a reasonable return on investment.

Since the time of our prior report, Congress has enacted the Consolidated Appropriations Act of 2016,[5] which prohibited the IRS from rehiring former employees without taking their prior conduct into account. In addition, during testimony before the Senate Finance Committee in February 2016, the IRS Commissioner was questioned regarding the IRS's process for rehiring employees previously fired for cause. During this testimony, the Commissioner explained that the employees mentioned in the prior TIGTA report were rehired under old hiring procedures, and would not be rehired under the IRS's updated procedures.

---

[4] TIGTA, Ref. No. 2015-10-006, *Additional Consideration of Prior Conduct and Performance Issues Is Needed When Hiring Former Employees* (Dec. 2014).
[5] Pub. L. No. 114-113, 129 Stat. 2242.

Given the substantial threat of identity theft and the magnitude of sensitive information that the IRS holds, hiring employees of high integrity is essential to maintaining public trust in tax administration and safeguarding taxpayer information. This is especially important in light of recent cyber events against the IRS intended to access tax information for the purposes of identity theft and filing fraudulent tax refunds. The IRS must ensure its systems and data are protected against both external and internal threats.

However, in a follow-up audit, TIGTA found that the IRS has not effectively updated or implemented hiring policies to fully consider past IRS conduct and performance issues prior to making a tentative decision to hire former employees, including those who were terminated or separated during an investigation of a substantiated conduct or performance issue.[6]

From January 1, 2015, through March 31, 2016, the IRS hired nearly 7,500 employees, of which more than 2,000 had been previously employed by the IRS. Although most employees who were rehired did not have prior conduct or performance issues, TIGTA found that more than 200 (approximately 10 percent) of the more than 2,000 rehired IRS employees were previously terminated from the IRS or separated while under investigation for a substantiated conduct or performance issue. More than 150 of these employees (approximately 75 percent) were seasonal. Four of the more than 200 employees had been terminated or resigned for willful failure to properly file their Federal tax returns; four separated while under investigation for unauthorized accesses to taxpayer information; and 86 separated while under investigation for absences and leave, workplace disruption, or failure to follow instructions. Some of these employees held positions with access to sensitive taxpayer information, such as contact representative positions.

Some rehired employees had past performance issues. For example, two rehired employees were previously terminated for failure to maintain a successful level of performance in multiple critical job elements as tax examining technicians. However, both of these employees were rehired as tax examining technicians less than six months later. In addition, 60 of the 824 employees we identified in our prior report as having been rehired with prior substantiated employment issues between January 1, 2010, and September 30, 2013, were rehired again between January 1, 2015, and March 31, 2016. Of these 60 employees, five had additional documented conduct or performance issues substantiated within nine days to 19

[6] TIGTA, Ref. No. 2017-10-035, *The Internal Revenue Service Continues to Rehire Former Employees With Conduct and Performance Issues* (July 2017).

months after being rehired. Three of the employees had the same issue in their prior employment.

Although the IRS follows specific criteria to disqualify applicants for employment, past IRS employment history is not provided to the selecting official for consideration when making a tentative hiring decision. IRS officials stated that it would be cost prohibitive to review prior issues before a hiring decision and tentative offer has been made. However, the IRS was unable to provide documented support for this position. In addition, TIGTA could not verify that the IRS always considered prior issues because reviews are not always documented. TIGTA also found that 27 former employees failed to disclose a prior termination or conviction on their application as required, but were still rehired by the IRS.

Although the IRS may have had a valid basis to rehire some of the more than 200 former employees with prior conduct or performance issues, TIGTA has serious concerns about the IRS's decision to rehire certain employees, such as those who willfully failed to meet their Federal tax responsibilities.

TIGTA recommended that the IRS Human Capital Officer provide the selecting official with access to records of former employee conduct and performance issues, and require that the basis for rehiring employees with prior employment issues be clearly documented. In their response, IRS management agreed with the intent of the recommendations and plans to update current practices and policies to ensure that data reflecting prior performance and misconduct are utilized in the hiring process.

INFORMATION SECURITY OVER TAXPAYER DATA

The IRS relies extensively on its computer systems to support both its financial and mission-related operations. These computer systems collect and process large amounts of taxpayer data. Recent cyber events against the IRS have illustrated that bad actors are continually seeking new ways to attack and exploit these IRS systems and processes in order to access tax information for the purposes of identity theft and filing fraudulent tax refunds. From the exploitation of IRS's Get Transcript application to that of the Data Retrieval Tool, the IRS has found that with each systemic weakness it closes criminals have discovered another means to access tax information from the IRS. In addition, the recent breach at Equifax that exposed sensitive personal information, including Social Security Numbers (SSN), could increase the risk of identity theft. As the threat landscape continues to evolve, we believe that protecting the confidentiality of taxpayer information will continue to be a top concern for the IRS.

TIGTA has assessed the IRS's electronic authentication platforms and made recommendations to develop a Service-wide strategy that establishes consistent oversight of all authentication needs across the IRS's functions and programs, ensures that the level of authentication risk for all current and future online applications accurately reflects the risk to the IRS and taxpayers should an authentication error occur, and ensures that the authentication processes meet Government Information Security Standards.[7] The IRS continues to take steps in response to TIGTA's recommendations to provide more secure authentication, including the implementation of two-factor authentication and the strengthening of application and network controls.[8] However, we remain concerned about the IRS's logging and monitoring capabilities over all connections to IRS online services. TIGTA is currently assessing the IRS's efforts to improve its authentication processes and has identified areas in which the IRS still needs improvement.[9] Specifically, the IRS has still not fully implemented network monitoring tools designed to improve prevention and detection of automated attacks and is not effectively monitoring audit logs for suspicious activity. Due to the importance of secure authentication of individuals' identities, we are planning to conduct additional reviews in this area.

The risk of unauthorized access to tax accounts will continue to be significant as the IRS proceeds with its Future State initiative,[10] which includes expansion of online tools it makes available to taxpayers. The IRS's goal is to eventually provide taxpayers with dynamic online tax account access that includes viewing their recent payments, making minor changes and adjustments to their tax accounts, and corresponding digitally with the IRS. Increased online access will increase the risk of unauthorized disclosure of tax data. As such, the IRS's processes for authenticating individuals' identities must promote a high level of confidence that tax information and services are provided only to individuals who are entitled to receive them.

---

[7] TIGTA, Ref. No. 2016-40-007, *Improved Tax Return Filing and Tax Account Access Authentication Processes and Procedures Are Needed* (Nov. 2015).
[8] TIGTA, Ref. No. 2016-20-082, *Improvements Are Needed to Strengthen Electronic Authentication Process Controls* (Sept. 2016).
[9] TIGTA, Audit No. 201720004, *Review of E-Authentication to IRS Online Services*, report planned for December 2017.
[10] Preparing the IRS to adapt to the changing needs of taxpayers is described generally as the IRS Future State initiative. A key part of this effort is for taxpayers to have a more complete online experience for their IRS interactions.

MODERNIZATION EFFORTS TO REPLACE LEGACY SYSTEMS

Successful modernization of IRS systems and the development and implementation of new information technology applications are critical to meeting the IRS's evolving business needs and to enhancing services provided to taxpayers. The IRS's reliance on legacy (*i.e.,* older) systems, aged hardware, and outdated programming languages pose significant risks to the IRS's ability to deliver its mission. Modernizing the IRS's computer systems has been a persistent challenge for several decades and will likely remain a challenge for the foreseeable future.

One of the IRS's top-priority information technology investments is the Customer Account Data Engine 2 (CADE 2). The IRS has been using the Individual Master File (IMF), which uses an outdated assembly language code, for more than 50 years. The IMF is the source for individual taxpayer accounts. Within the IMF, accounts are updated, taxes are assessed, and refunds are generated. Most of the IRS's information systems and processes depend, directly or indirectly, on the IMF.

In 2009, the IRS began developing CADE 2 to address the issues regarding tax processing and to eventually replace the IMF. According to the IRS, CADE 2 is the data-driven foundation for future state-of-the-art individual taxpayer account processing and data-centric technologies designed to improve service to taxpayers, enhance IRS tax administration, and ensure fiscal responsibility.

In September 2013, TIGTA reported that the CADE 2 database could not be used as a trusted source for downstream systems because of the 2.4 million data corrections that had to be applied to the database and the IRS's inability to evaluate 431 CADE 2 database columns of data for accuracy.[11] To address these issues, the IRS developed additional tools and implemented a new data validation testing methodology intended to ensure CADE 2's timeliness, accuracy, integrity, validity, reasonableness, completeness, and uniqueness. The IRS requested that TIGTA evaluate the new data validation testing methodology.

In a September 2014 follow-up audit, TIGTA reported that the IRS had appropriately completed its data validation efforts.[12] According to the IRS, the CADE 2 release plan is currently being adjusted to reflect impacts of staffing challenges and

---

[11] TIGTA, Ref. No. 2013-20-125, *Customer Account Data Engine 2 Database Deployment Is Experiencing Delays and Increased Costs* (Sept. 2013).
[12] TIGTA, Ref. No. 2014-20-063, *Customer Account Data Engine 2 Database Validation Is Progressing; However, Data Coverage, Data Defect Reporting, and Documentation Need Improvement* (Sept. 2014).

various possible budget scenarios. The loss of key IMF expertise is causing the reprioritization of CADE 2 goals to focus on IMF reengineering, the suspension of projects, and the potential deferral of planned functionality to be delivered. There are several reasons for the delays in implementing CADE 2, including other organizational priorities such as the annual filing season, other major information technology investments, contracting delays, aging architecture, lack of key subject matter experts on institutionalized processes, and outdated programming languages. There is no scheduled or planned completion date for CADE 2 development.

In FY 2018, TIGTA will be initiating an audit to assess the effect of legacy systems on the IRS's ability to deliver modernized tax administration. TIGTA also plans to conduct an audit to determine the progress made on completing the CADE 2 project, including the IRS's retirement strategy for the IMF and a comparison of estimated costs to actual expenditures.

INFORMATION TECHNOLOGY INITIATIVES TO MODERNIZE THE E-MAIL SYSTEM

In addition to modernization efforts to replace legacy systems, the IRS is developing and implementing new information technology to modernize its operations, applications, and e-mail system to provide more sophisticated tools to taxpayers and IRS employees. TIGTA has identified several areas where the IRS can improve its efforts to upgrade or enhance its information technology systems.

For example, TIGTA has evaluated the IRS's efforts to establish information technology capabilities to manage temporary and permanent e-mail records. TIGTA determined that the IRS purchased subscriptions for an enterprise e-mail system it could not use.[13] The purchase was made without first determining project infrastructure needs, integration requirements, business requirements, security and portal bandwidth, and whether the subscriptions were technologically feasible on the IRS enterprise. IRS executives made a management decision to consider the enterprise e-mail project an upgrade to existing software instead of a new development project or program. As a result, the IRS did not follow its Enterprise Life Cycle guidance. The IRS authorized the $12 million purchase of subscriptions over a two-year period; however, the software to be used via the purchased subscriptions was never deployed. The IRS violated Federal Acquisition Regulation requirements by not using full and open competition to purchase the subscriptions.

[13] TIGTA, Ref. No. 2016-20-080, *Review of the Enterprise E-mail System Acquisition* (Sept. 2016).

In an audit requested by the Chairman of the House Committee on Ways and Means and the Chairman of the Senate Committee on Finance, TIGTA determined that IRS policies are not in compliance with Federal electronic records requirements and regulations.[14] At the time of that report, TIGTA found that the IRS's current e-mail system and record retention policies did not ensure that e-mail records were automatically archived for all employees and could be searched and retrieved for as long as needed. The e-mail system in place at that time required users to take manual actions to archive e-mail and resulted in e-mail records that were stored in multiple locations, such as mailbox folder, Exchange server, network shared drive, hard drive, removable media, or backup tape.

According to the IRS, its Future State e-mail system, which was planned to be implemented by September 30, 2017, was developed to potentially allow records to be available and searchable while automatically applying a retention policy. However, until a solution is effectively implemented, IRS e-mails remain difficult, if not impossible, to retain and search.

TIGTA has also evaluated the readiness of the IRS to establish an upgraded e-mail solution with the information technology capabilities to manage e-mail records in compliance with the directive of the Office of Management and Budget (OMB) and the National Archives and Records Administration (NARA), which requires that agencies eliminate paper records and use electronic recordkeeping to the fullest extent possible.[15] TIGTA found that more effort is needed by the IRS to meet the NARA e-mail management success criteria prior to the deployment of the enterprise e-mail solution. Specifically, TIGTA determined that as of January 31, 2017, 13 of the 32 (41 percent) requirements related to the e-mail management success criteria remained under development. The requirements need to be fully developed and implemented before the IRS can successfully deploy its enterprise e-mail solution. Due to delays in developing and deploying the enterprise e-mail solution, the IRS will most likely not begin receiving any of the expected benefits of Federal records reform until the end of Calendar Year 2017, nearly a year after the initially mandated deployment date.

[14] TIGTA, Ref. No. 2017-10-034, *Electronic Record Retention Policies Do Not Consistently Ensure That Records Are Retained and Produced When Requested* (July 2017).
[15] TIGTA, Ref. No. 2017-20-039, *Additional Efforts Are Needed to Ensure the Enterprise E-Mail Records Management Solution Meets All Requirements Before Deployment* (Aug. 2017).

HARDWARE MODERNIZATION

The IRS has a large and increasing amount of aged hardware, some of which is three to four times older than industry standards. In its FY 2016 President's Budget Request, the IRS noted that its information technology infrastructure poses significant risk of failures, although it is unknown when these failures will occur, how severe they will be, or whether they will have material impacts on tax administration during the filing season.

TIGTA conducted an audit to determine and measure the impact of inefficiencies of the IRS's aged information technology hardware. Specifically, TIGTA analyzed all FY 2016 incident tickets[16] from the Knowledge Incident/Problem Service Asset Management system[17] categorized as either "critical" or "high" for all aged information technology hardware (*e.g.,* desktop and laptop computers, servers, and telephone call routers). The aggregate length of time to resolve these incident tickets was 4,541 hours. Aged information technology hardware still in use could result in excessive system downtime due to hardware failures. As information technology hardware ages, it becomes more difficult to obtain adequate support. Aged hardware failures have a negative impact on IRS employee productivity, the security of taxpayer information, and customer service.

Additionally, TIGTA reported that the IRS has not yet achieved its stated objective of reducing the percentage of its aged information technology hardware to an acceptable level of 20 to 25 percent. In fact, the IRS's percentage of aged information technology hardware has steadily increased from 40 percent at the beginning of FY 2013 to 64 percent at the beginning of FY 2017.[18] Aged information technology hardware, when combined with the fact that components of the infrastructure and systems are interrelated and interdependent, make outages and failures unpredictable and may also introduce security risks to critical taxpayer data that IRS systems must protect.

---

[16] Incident tickets are created as part of the IRS's Information Technology Incident Management Process that defines the process and procedures for recording, categorizing, prioritizing, investigating, diagnosing, resolving, dispatching, monitoring, and closing out the incidents.

[17] This system maintains the complete inventory of information technology and non-information technology organization assets, computer hardware, and software. It is also the reporting tool for problem management with all IRS-developed applications and shares information with the Enterprise Service Desk.

[18] TIGTA, Ref. No. 2017-20-051, *Sixty-Four Percent of the Internal Revenue Service's Information Technology Hardware Infrastructure Is Beyond Its Useful Life* (Sept. 2017).

IRS USE OF CRITICAL PAY AUTHORITY

Over the course of the last three years, some Federal Government agencies have suffered significant cyber data breaches. Both the OPM and the IRS were included in the list of *Network World's* "Biggest Data Breaches of 2015."[19] Efforts to exploit cyber systems by various means have highlighted the need for agencies to seek the capacity to improve existing systems or build new ones. One element associated with building that capacity is hiring individuals with proven skills, knowledge, and abilities related to systems design and cybersecurity. The same skills are also highly desired in the private sector. Federal agencies generally have fewer hiring compensation flexibilities than the private sector when seeking well-qualified employees.

This issue is not new, and in 1990 the Critical Position Pay Authority (CPPA) was codified in 5 U.S.C. § 5377. This authority allows agencies to seek the approval of the OPM and the OMB to pay annual salaries up to the Executive Schedule Level I of $207,800 (in 2017) for approved staff members versus $187,000 for employees of the Senior Executive Service (SES).[20]

For an employee to receive critical position pay, he or she must be considered well-qualified for the position. In addition, critical pay positions require an extremely high level of expertise in a scientific, technical, professional, or administrative field and must be critical to the successful accomplishment of the agency's mission.

In 1998, Congress provided the IRS its own Streamlined Critical Pay (SCP) authority.[21] Similar to the CPPA, the IRS would be allowed to pay salaries higher than the limit applied to employees in the SES and those in the Executive Schedule Level I. The SCP authority allowed the IRS to quickly hire and retain employees and compensate these employees up to the salary level of the United States Vice President, which in 2017 is $240,100. The IRS was limited to a maximum of 40 SCP employees on roll at any one time. Significantly, the IRS was not required to seek approval from the OPM and the OMB to hire and determine the salary for individuals hired for SCP positions. For this reason, the authority was considered streamlined.

---

[19] Tim Greene, Year in Review 2015: Biggest data breaches of 2015, Network World (Dec. 2, 2015, 10:12 AM), https://www.networkworld.com/article/3011103/security/biggest-data-breaches-of-2015.html.
[20] As of January 2017, for employees of Federal agencies with a certified SES performance appraisal system, the maximum salary is $187,000.
[21] IRS Restructuring and Reform Act of 1998 (RRA 98), Pub. L. No. 105-206, 112 Stat. 685.

Congress extended the IRS's SCP authority on two occasions, and it eventually expired on September 30, 2013. On several occasions in 2015 and 2016, the IRS Commissioner remarked about the loss of SCP authority, and in an April 2016 congressional hearing noted the loss "has made it very difficult, if not impossible, to recruit and retain employees with expertise in highly technical areas such as information technology."[22] The IRS stated that no individuals remained employed with the IRS under the SCP authority. However, IRS management advised that 7 employees previously hired under SCP are currently employed with the IRS after being selected from competitive job vacancy announcements.

However, TIGTA reported that the IRS has not used the CPPA to hire employees.[23] IRS officials have not pursued use of the CPPA because they believed that the expired SCP authority would be restored. Compared to the SCP, the CPPA process requires additional layers of approval and offers substantially less pay flexibility. The SCP authority was delegated to the IRS Commissioner in 2009 and did not need Department of the Treasury, OPM, and OMB approval. While SCP authority is unavailable, use of the CPPA can provide the IRS an enhanced capability in its recruitment efforts. Specifically, the $207,800 salary available under the CPPA exceeds the $187,000 maximum that can be offered to career-level Federal executives.

TIGTA further found that the CPPA is not widely used among other Federal Government agencies. Within the Federal Government, a maximum of 800 employees can receive critical pay at any one time, but per the latest annual report from the OPM, in calendar year 2015 only four individuals were hired as CPPA employees. Our research showed that some of the reasons the CPPA was not widely used include the availability of other agency-specific pay authorities, the lengthy approval process, and cultural issues such as paying individuals more than their manager. In their response to our report, IRS management indicated that they will be seeking approval from the OPM and the OMB to use the CPPA to hire three Information Technology executives in the fields of data management, engineering, and architecture.

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 operate efficiently and effectively and to

---

[22] *Can the IRS Protect Taxpayers' Personal Information, Hearing Before the House Science, Space and Technology Committee, Subcommittee on Research and Technology,* 114th Cong. 22 (2016) (statement of John Koskinen, IRS Commissioner).
[23] TIGTA, Ref. No. 2017-IE-R007, *The Internal Revenue Service Has Not Used Critical Position Pay Authority to Hire Employees* (July 2017).

investigate any instances of IRS employee misconduct or other threats to tax administration.

Chairman Jordan, Chairman Meadows, Ranking Member Krishnamoorthi, Ranking Member Connolly, and Members of the Subcommittees, thank you for the opportunity to share my views.