May 3, 2017

Reviewing the FAFSA Data Breach

Committee on Oversight and Government Reform, United States House of Representatives, One Hundred Fifteenth Congress, First Session

---

Hearing Contents:

** Please Note: External links included in this compilation were functional at the time of its creation but are not maintained thereafter.*

Gina Garza
Chief Information Officer
Internal Revenue Service
View Testimony

Tim Camus
Deputy Inspector General
Treasury Inspector General for Tax Administration
View Testimony

Available Webcast(s)*:

Hearing Webcast

Compiled From*:

https://oversight.house.gov/hearing/reviewing-fafsa-data-breach/

** Please Note: External links included in this compilation were functional at the time of its creation but are not maintained thereafter.*

Written Testimony
James W. Runcie
Chief Operating Officer
Federal Student Aid
U.S. Department of Education

"Examining the Cybersecurity Incident that Affected the IRS Data Retrieval Tool"
Before the U.S. House of Representatives Committee on Oversight and Government Reform

May 3, 2017

Thank you, Chairman Chaffetz, Ranking Member Cummings, and members of the Committee, for the opportunity to join you today. I will discuss the events that led up to the security incident that precipitated the Internal Revenue Service (IRS) disabling the Data Retrieval Tool (DRT) on March 3, 2017. I also will discuss the plan the U.S. Department of Education (the Department) office of Federal Student Aid (FSA) and the IRS have to restore DRT functionality, as well as actions FSA has taken to assist impacted students, parents, borrowers, and postsecondary institutions.

FSA remains the largest source of Federal student aid for postsecondary education in the United States. In Fiscal Year 2016, FSA delivered nearly $125.7 billion in aid to more than 13 million students attending more than 6,000 postsecondary institutions. In response to legislative, regulatory, and policy changes, FSA has successfully implemented a number of major modifications to our operating environment. One of these developments is the implementation of the DRT, which first became available in 2010.

Background about the DRT

Section 6103 of the Internal Revenue Code/USC restricts the sharing of taxpayer information without their explicit consent. The DRT is a solution the IRS and the Department developed to fit the legal constraints around sharing tax information without explicit consent. The DRT is accessed via the *Free Application for Federal Student Aid* (FAFSA®) where the applicant can explicitly consent to receive their tax data and then electronically transfer that data into the FAFSA application. In essence, the DRT allows the data to electronically flow through the consumer before being transferred into the FAFSA.

The DRT is the result of a collaborative effort between the IRS and FSA, intended to provide students, parents, and borrowers an easy and effective method to access required IRS tax information and transfer that data directly from the IRS into a FAFSA or an income-driven repayment (IDR) plan application. Using the DRT saves time and ensures greater accuracy of applicants' information. Each year, approximately 20 million FAFSA forms are submitted. The most recent data indicate that roughly half of all FAFSA filers use the DRT to transfer their tax information from the IRS, and approximately 4.5 million borrowers use the DRT to transfer their tax information into an IDR plan application.

The existence of the DRT paved the way for two recent FAFSA simplification advancements aimed at reducing barriers to accessing a postsecondary education: the "Early" FAFSA and the use of "prior-prior" year tax information. Traditionally, the FAFSA is available each year on January 1.

Last year, however, FSA launched the 2017–18 FAFSA three months earlier—on October 1, 2016, rather than January 1, 2017—and required applicants to use tax return data from the prior-prior year (2015, not 2016). This change allowed more FAFSA filers to use the DRT, provided students and families with financial aid information earlier to consider in their selection of schools, and allowed applicants to submit a FASFA without having to return to the application in order to correct it after they filed their tax return.

The DRT serves as an important program integrity measure, as well. We know that filers may sometimes incorrectly enter their information into the FAFSA, which may result in improper payments. The DRT essentially eliminates the chances of this type of user error-generated improper payment. It also reduces the need for a secondary program integrity measure. Postsecondary institutions are required to verify certain information from the FAFSA for any applicant who has been selected by the Department for such verification. Nationally, using a risk-assessment regression analysis, the Department selects between 25 and 30 percent of FAFSA filers for verification. Verification requires applicants to provide documentation to their institution—including IRS tax return information—to confirm what was provided by the applicant when completing the FAFSA. For applicants who use the DRT, institutions can rely on the information obtained from the IRS, thereby eliminating the burden associated with manually verifying information students and parents reported. While the DRT was operational, the Department saw decreases in verification rates from the prior year of approximately seven percentage points.

IRS and FSA Joint Efforts to Increase Security of the DRT

In October 2016, the IRS contacted FSA about a potential vulnerability it identified with the DRT as a result of a broader review IRS had undertaken assessing all the ways taxpayers and others interact with IRS' systems. FSA sought to determine the best approach to minimize the vulnerability without causing a major disruption to students, parents, and borrowers. To avoid negative impacts to students, parents, and borrowers, the IRS and FSA agreed to keep the DRT operational while the IRS increased monitoring of the tool for any suspicious activity. The increased monitoring was intended to reduce the risk of exposing tax return information and other personally identifiable information (PII) associated with the DRT without limiting access to the FAFSA and IDR plan applications for a significant segment of students and families.

Since October, the IRS and FSA have evaluated nearly one dozen potential options– capable of being integrated with the FAFSA and IDR plan applications—to increase the protection of taxpayer information on the DRT; options considered include different versions of data masking, slight data modification, higher levels of authentication, or a legislative change to Internal Revenue Code section 6103 that would authorize the Department of Education to securely receive the data directly from the IRS. While we hoped to be able to implement a solution to prevent any disruption to the DRT, evaluating options was crucial in being able to move toward the option we will implement for the 2018–19 FAFSA cycle.

Analyzing and Investigating the Suspicious Activity Related to the DRT

By early March, the IRS identified suspicious activity related to the DRT. On March 3, 2017, the IRS alerted FSA, suspended the use of the DRT, and placed an outage message on the DRT website.

There is no evidence that the malicious actors accessed any personal information from the Department's systems. We are confident that the personal information the Department has on borrowers, students, and parents remains appropriately protected. While the FAFSA was involved, FSA believes this was, in essence, a scheme directed at retrieving tax data from the IRS. Using personal information obtained illegally from other sources—including name, Social Security number, date of birth, address, and tax filing status—malicious actors were able to start filling out FAFSAs. The malicious actors then used the DRT to access taxpayer information from the IRS, including the Adjusted Gross Income, which is necessary to file a fraudulent tax return.

FSA provided the IRS with a preliminary analysis related to the list of potentially impacted taxpayers, which included transactional data from FSA systems, to assist the IRS in reconciling conclusions with its own ongoing analysis. On April 3, 2017, the IRS informed FSA that it was treating the security incident as a "major" incident as defined under the Office of Management and Budget's (OMB) guidance in OMB M-17-12.

The Department continues to review data from the IRS to take necessary administrative action to protect applicant data and taxpayer funds. We are cooperating with the Office of Inspector General and will keep it fully informed as it proceeds with its joint criminal investigation with the Treasury Inspector General for Tax Administration.

Communications to Students, Parents, Borrowers, and Others

FSA recognizes the widespread concern about how the unavailability of the DRT has affected those Americans we serve—particularly those who are from low-income backgrounds or who are first-generation college applicants—and the postsecondary institutions they attend. We remain steadfast in our efforts to fulfill our mission of providing access to higher education for all Americans while protecting sensitive student, parent, and borrower information. We are committed to doing all that we can to help students, parents, and borrowers successfully submit applications by manually providing their tax return information while the DRT is unavailable.

Since the DRT was disabled on March 3, 2017, FSA has provided guidance to the public on multiple platforms indicating that students, parents, and borrowers can still apply for federal student aid and repayment plans. Information also explains how to apply while the tool is unavailable.

The IRS and FSA have released two joint statements—on March 9 and March 30—that inform the public (1) that tax information can be provided manually on both the FAFSA and IDR plan application websites and (2) how to obtain copies of their tax returns, if they are unable to access their own copies. Information about the status of the DRT has been posted to FSA's Information for Financial Aid Professionals (IFAP) website—ifap.ed.gov—which serves as the primary information portal for financial aid professionals, and to StudentAid.gov, FSA's flagship information portal for students, parents, and borrowers.

The March 30 announcement on StudentAid.gov includes detailed instructions about completing a FAFSA without access to the DRT, along with an easy-to-follow table showing which line to reference for specific tax information, depending on which IRS tax form the student or parent filed.

Other ways FSA has shared information to help students, parents, borrowers, and institutions, include:

- Providing FSA customer contact centers with information to explain how students, parents, and borrowers should manually provide tax information for the FAFSA and IDR plan applications. Customer service representatives at the Federal Student Aid Information Center currently are fielding approximately 500 more customer inquiries per day related to the DRT than before the tool was disabled.

- Posting an announcement on its fafsa.gov home page that includes a reminder that information can be entered manually on the application, and FSA links directly to guidance available on the IRS's website that provides students, parents, and borrowers with instructions for obtaining a tax return transcript.

- Using social media applications, Facebook and Twitter, to encourage students, parents, and borrowers to apply for aid by manually providing their tax information. Such messaging via social media has been shared broadly by college access organizations that help support FSA's mission.

- Posting on the Financial Aid Toolkit—a website that provides information for counselors and college access mentors—with links to other related information, making it easy for counselors and mentors to share information with the students they support.

- Emailing approximately 2,000 partner organizations—including counselors, mentors, and financial aid professionals—informing them to plan for the DRT to be unavailable until fall 2017, the beginning of the next FAFSA season.

- Notifying financial aid professionals directly via an Electronic Announcement to schools. The communication advises institutions that the online applications remain operational and that applicants should manually provide financial information from copies of their tax returns.

- Adding language to the IDR plan application informing borrowers that servicers can accept documentation of income by fax or mail, or that they may upload proof of income documents directly and securely through servicers' websites. Contact centers and FSA training officers have been also notified of the additional language.

- Sending a memo to state grant agencies encouraging them to consider providing flexibilities related to application deadlines or other administrative requirements for students and families who may need more time to apply for aid while the DRT is unavailable.

- Issuing a Dear Colleague Letter to postsecondary institutions extending flexibilities institutions may choose to use as part of their verification procedures. These flexibilities begin immediately and apply to both the 2016–17 and 2017–18 FAFSA processing and verification cycles.

At the end of March, FSA provided briefings to staff of several congressional committees, including this committee, the Senate Committee on Homeland Security and Governmental Affairs, the Senate Committee on Finance, the House Committee on Ways and Means, and the Senate Committee on Health, Education, Labor and Pensions. We will continue to be accessible to you and provide

answers to your questions as we work toward making the FAFSA accessible to everyone who wants to go pursue a postsecondary education while protecting sensitive taxpayer data.

The Encryption Solution

In an effort to determine an acceptable solution to a vulnerability related to the DRT, as previously stated, on February 9, 2017, the IRS and FSA agreed to pursue an encryption solution. This solution provides potentially the best balance between securing personal information and access to financial aid under current law and in time for the next federal student aid application cycle, which starts on October 1. The DRT returns 11 taxpayer data elements to the FAFSA and four data elements to the IDR application. The solution will encrypt the taxpayers' information and hide it from applicants' view on the IRS DRT web page, as well as on the FAFSA and IDR plan application web pages. While students, parents, and borrowers will still be able to electronically transfer their own data into a FAFSA or an IDR plan application, taxpayer information will no longer be visible to would-be malicious actors. We acknowledge some filers may have concerns about not being able to see the information they are transferring from the IRS into the FAFSA. We will continue to work with the financial aid community and the IRS to address these concerns.

FSA and the IRS have been working together to expedite the implementation of the encryption solution. The IRS, which had to modify four basic input and output web pages and supporting processes, implemented the majority of the solution in March in a configurable way, which allowed the IRS to turn it on or off separately for the IDR plan application and the FAFSA.

To implement the encryption solution, FSA must re-engineer the IDR plan application and FAFSA application processes. And because process changes to both applications significantly impact other parts of the financial aid ecosystem—students, parents, borrowers, postsecondary institutions, state grant agencies, and servicers, among others—the changes and impacts must be carefully communicated in a thorough, deliberate manner. Obscuring taxpayer information in the FAFSA process will require additional assistance from postsecondary institutions.

Currently, FSA and the IRS are working toward a goal to implement the encryption solution by the end of May or early-June for the IDR plan application. FSA's implementation of the solution for the FAFSA, however, is more complicated.

Each award year involves a separate FAFSA implementation. Presently, there are two active FAFSA cycles:

1. The 2016–17 FAFSA cycle, which began January 1, 2016, and extends until June 30, 2017, when no new applications will be accepted; and
2. The 2017–18 FAFSA cycle, which began October 1, 2016, and extends until June 30, 2018.

The 2018–19 FAFSA cycle will begin October 1, 2017, and will extend until June 30, 2019. The implementation of the 2018–19 FAFSA began in August 2016.

Over the years, FSA has worked to simplify the experience for the FAFSA filer; despite relatively complex program requirements. FSA has implemented improvements to the FAFSA, including skip logic, multiple external interfaces, and hundreds of validation edits in order to assist applicants or to reduce the number of questions posed to applicants, based on their individual circumstances. As would be expected, any time a change is made to the FAFSA process, a significant amount of testing must occur to ensure that the process and supporting web pages operate as intended.

When FSA and the IRS agreed to the encryption solution, FSA had to compress the 2018–19 FAFSA implementation schedule by three months in order to implement the 2018–19 FAFSA by October 1, 2017, as planned. We will implement by that date, and the 2018–19 FAFSA cycle will include the encryption solution.

The earliest possible timeframe to implement the solution for the 2017–18 FAFSA cycle would have been October 1, 2017. By that time, we estimate that 92 percent of the expected 2017–18 FAFSA filers would already have submitted their applications; before the DRT was disabled, approximately 4.7 million 2017–18 FAFSA applicants used the tool.

More critically, in order to implement the solution by October 1 for the 2017–18 FAFSA cycle, FSA would have needed to divert contractor expertise, technical resources, and Federal subject matter experts from the upcoming 2018–19 FAFSA implementation. Striving to make the DRT available to the remaining eight percent of 2017–18 FAFSA filers would have introduced an unacceptable level of risk to the applicants relying on the 2018–19 FAFSA launch. Such a diversion of resources would have significantly increased the likelihood of flaws in the 2018–19 FAFSA implementation or would have caused the 2018–19 FAFSA to be launched after October 1. Diverting resources also could have impacted application processing, resulting in delays in institutions and students accessing Federal loan, grant, and work study funds. Therefore, the DRT will remain unavailable and the encryption solution will not be implemented for the remainder of the 2017–18 FAFSA cycle.

Conclusion

For several months, FSA and the IRS have been working collaboratively to address an identified vulnerability with the DRT, investigate the related security incident, implement short-term solutions, and discuss other options for long-term solutions that ensure that the FAFSA remains accessible to everyone who wants to go to college while protecting sensitive taxpayer data. As FSA works to implement the encryption solution by the end of May or early-June for the IDR plan application and by October 1 for the 2018–19 FAFSA, we also have begun developing comprehensive communications plans for students, parents, borrowers, postsecondary institutions, and others about the solution. We continue to work with the IRS to implement the encryption solution, because we understand that the protection of individuals' personal information is critically important and share the IRS' commitment to make information security a high priority.

I appreciate the opportunity to provide the Committee with an overview of events that precipitated the IRS disabling the DRT, actions FSA has taken to assist impacted students, parents, borrowers, and institutions, and the plan to implement the encryption solution. I welcome any questions you may have today.

James W. Runcie, Chief Operating Officer, Office of Federal Student Aid — Biography

Former U.S. Secretary of Education Arne Duncan appointed James W. Runcie as the Chief Operating Officer (COO) for the Office of Federal Student Aid (FSA) on September 15, 2011. FSA is the federal government's first Performance-Based Organization established as part of the *Higher Education Amendments of 1998* to modernize the delivery of student financial assistance, and improve service to millions of students and the postsecondary institutions they attend.

The COO advises the Secretary of Education on matters related to the U.S. Department of Education's operation of student financial assistance programs under *Title IV* of the *Higher Education Act of 1965*, as amended.

As COO, Mr. Runcie is responsible for the strategic and operational management of FSA. Since 2010, FSA has managed an unprecedented increase in the student loan portfolio from approximately 9.2 million recipients with $155 billion of William D. Ford Federal Direct Loan Program (Direct Loan), to 32 million recipients with $1 trillion of Direct Loans today. The overall portfolio is approximately $1.3 trillion with more than 42 million borrowers. Despite this growth, the portfolio performance has improved substantially with cohort default rates dropping more than 20% in the most recent three years, and over 43% of the Direct Loan portfolio dollars in income driven repayment plans. On an annual basis, FSA originates and disburses approximately $125 billion of loans and aid to approximately 13 million students attending over 6,000 colleges and institutions of higher education. FSA comprises numerous operating units and divisions reporting to the COO. These include product management and servicing, customer experience, enterprise data research and analytics, risk management, acquisitions, compliance, enforcement, finance, technology, project management, communications and outreach, administrative services and strategic planning. FSA has an operating budget of approximately $1.6 billion and more than 13,000 employees and contractors.

Prior to managing FSA, Mr. Runcie garnered 20 years of experience in the banking sector, working with major financial institutions, including UBS Investment Bank, Banc of America Securities (Bank of America), and Donaldson, Lufkin & Jenrette (Credit Suisse). His duties included transaction management and execution, project management, business development, group operations, marketing, human resources and risk management. Mr. Runcie also worked on a broad range of services, including public and private capital raising, mergers and acquisitions, merchant banking, debt-equity-hybrid structures and general advising. He also worked within numerous industries, including technology, internet, financial, industrial, casino and gaming, healthcare, agribusiness, sports, retail, toy and others. Assignments included transactions and advisory work in North America, Latin America, Europe and Asia. Prior to his banking experience, Mr. Runcie was a systems consultant in the network division of Xerox Corporation.

Mr. Runcie holds a Bachelor's of Arts in Mathematics from the College of the Holy Cross and a Master's of Business Administration, with distinction, from Harvard Business School.

Written Testimony
Jason K. Gray
Chief Information Officer
U.S. Department of Education

"Examining the Cybersecurity Incident that Affected the IRS Data Retrieval Tool"
Before the U.S. House of Representatives Committee on Oversight and Government Reform

May 3, 2017

Good morning Mr. Chairman, Ranking Member Cummings, and Members of the Committee. I am Jason Gray, Chief Information Officer (CIO) for the U.S. Department of Education ("Department"), a position I have had the privilege of holding since June, 2016.

I appreciate the opportunity to speak with you today on the cybersecurity incident that affected the Internal Revenue Service (IRS) Data Retrieval Tool (DRT), specifically, the operational and cybersecurity decisions before and after the tool was taken offline. As the CIO, I embrace and support the Department's mission of *promoting student achievement and preparation for global competitiveness, fostering educational excellence and ensuring equal access*, by ensuring that we apply information technology (IT) effectively, efficiently, and securely. I take this responsibility seriously, and understand that this includes the entire Department, including Federal Student Aid (FSA) and all principal and support offices.

On March 3, 2017, I became aware that the IRS had confirmed that tax data accessed through the FAFSA DRT may have been used to fraudulently file tax returns. The Department's Security Operations Center (EDSOC) was notified about suspicious behavior on the IRS DRT on March 3, 2017. The DRT is an IRS tool leveraged by the Department's Free Application for Federal Student Aid (FAFSA) by allowing applicants to access required parts of their tax information

electronically for them to insert into their student aid applications. We immediately activated our incident response processes, beginning with actions to understand details of the events that occurred, and to identify appropriate responses. This involved coordination of Security Operations Center resources to gather forensic data and to gain a fuller understanding of the incident. We held daily meetings to facilitate communication between the technical staff of the Office of the Chief Information Officer (OCIO), FSA, and the IRS. Additionally, we reported the incident to our Office of the Inspector General and to the United States – Computer Emergency Readiness Team (US-CERT) at the Department of Homeland Security (DHS) on March 3, 2017, and March 4, 2017, respectively. While the Department's systems were involved, this was, in essence, a scheme directed at retrieving tax data from the IRS. The malicious actors used stolen PII to start FAFSA forms in order to obtain information from the IRS to attempt to file fraudulent tax returns. There is no evidence that the malicious actors were able to access any personal information held on the Department's systems. We are confident that the personal information the Department has on borrowers, students, and parents remains appropriately protected.

This issue, which involved the unlawful use of a Department system by outside parties, underscores the need for the Department to be continually vigilant in the operation and improvement of our cybersecurity capabilities. Toward that end, we have undertaken multiple projects to improve capabilities consistent with Industry Best Practices and the National Institute of Standards and Technology (NIST) Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover). The Cybersecurity Framework applies the principles and best practices of risk management to improving the security and resilience of critical infrastructure. I will describe

several actions we have taken to further strengthen and enhance our cybersecurity program to protect sensitive data, including PII that is managed by the Department.

Incident Response

Incident response is a priority for the Department. In 2015 we created an Incident Response Planning Workgroup to address cybersecurity incidents and data breach response processes with separate work streams for communications, breach response planning, and privacy and legal. This group validated the mapping of key network systems, revised agency policies and directives as needed, evaluated and identified necessary amendments to the security clauses in vendor contracts, and developed technical and procedural protocols to guide decision-making in the event of a breach.

In Fiscal Year (FY) 2016, the Department conducted two incident response table-top exercises that helped us refine our incident response process through the development of lessons learned and identification of actions the Department needed to enhance our overall incident response processes. We have taken all actions identified in the two FY 2016 tabletops and plan multiple tabletops in FY 2017 as well.

Additionally, with the publication of the FY 2017 Inspector General Federal Information Security Modernization Act (FISMA) Reporting Metrics, the Department has performed a self-assessment against the Incident Response metric area. The Department is currently working to incorporate additional measures to achieve at least "Level 2" status across our Incident Response

program, to include the consolidation of our Security Operations Center capabilities, processes, and resources.

Internal Technical Controls

The Department has implemented a number of technical controls and solutions to detect policy violations, unauthorized changes, and unauthorized access to the Department's primary network. These include a Data Loss Prevention (DLP) solution, which went live in October of 2016 that restricts users from sending emails that contain sensitive PII, such as social security numbers, outside of the Department. In 2016 the Department also implemented Network Access Control (NAC), which allows for validation of the security posture of all endpoints against standard Department cybersecurity policies, and prevents the connection by any unauthorized device to the network. A third solution, Web Application Firewalls (WAFs), has been implemented and we are transitioning web portals and web applications to be protected by the WAFs.

The Department continues to focus on achieving Federal goals for strong authentication, as 100 percent of privileged users, and over 85 percent of our non-privileged users are required to use their Personal Identity Verification (PIV) card in order to log on to the Department's network.

Outreach and Collaboration with DHS

The Department has partnered with DHS on the implementation of automated solutions for Continuous Diagnostics and Mitigation (CDM), which will enable us to continuously monitor our network for intrusions and malicious activity. The Department also actively leverages DHS-provided shared security services such as EINSTEIN 3A tools for threat analysis and threat

indicators, US-CERT surge support for forensics analysis, and High Value Asset assessments.

The Department is also working in other ways to help ensure only authorized users are accessing the Department's systems and data. The FSA ID—a user-selected username and password—is required for students, parents, and borrowers to authenticate their identity and access their federal student aid information online. The websites that require an FSA ID to log in are fafsa.gov, NSLDS Student Access, StudentAid.gov, StudentLoans.gov, and the Federal Student Aid Feedback System (when a customer chooses to authenticate). Since the implementation of the FSA ID almost two years ago, over 45 million people have successfully created an FSA ID and have used their FSA IDs to log in over 315 million times. Recently the Department announced an additional disclaimer prior to log-in that will warn against unauthorized usage of the FSA ID by third-party for-profit entities. The user must select "Accept" in order to proceed.

While the Department has taken a number of positive steps to prevent the unauthorized access and loss of sensitive data, we recognize that there is still work to be done. The Department has fully embraced and is leveraging the mandates of the Federal Information Technology Acquisition Reform Act (FITARA), which we believe is prudent to continually improve and mature our processes in the realm of overarching IT Security and Governance.

Conclusion

I thank you for the opportunity to discuss the cybersecurity incident that affected the DRT, and the operational and cybersecurity decisions made before and after the tool was taken offline. The Department of Education and the IRS continue working together at all appropriate levels to

significantly improve the security and privacy protections around this important capability. I am confident that the technical solution currently being worked will achieve this goal. I would be pleased to answer any questions you may have.

Jason K. Gray, Chief Information Officer, U.S. Department of Education – Biography

Jason K. Gray was selected in May 2016 to serve as the U. S. Department of Education's Chief Information Officer (CIO). In this position he oversees an information technology (IT) portfolio of $689 million in programs. As the CIO, Gray serves as a principal advisor to the Under Secretary, Deputy Secretary, and Secretary with respect to the astute use of IT to exceed the expectations of the Department's customers. He serves as the day-to-day lead for coordinating and managing the various functions within Office of the Chief Information Officer, coordinates with and provides advice to the Department's senior leadership regarding IT, information management, information assurance, and website activities management and operations.

Prior to his selection as CIO, Gray served as the Associate Chief Information Officer for the Department of Transportation (DOT), where he provided executive leadership on IT policy and oversight for information governance, compliance, and departmental policy, as well as managed DOT's $3.5 billion IT portfolio.

Gray has held several leadership roles in the information technology and healthcare administration fields. He has nearly 20 years of experience in the planning, development, delivery, and monitoring of technical solutions that address the needs of his customers in support of their missions.

Gray received his M.B.A. from Colorado Technical University, completed the Key Executive Leadership Certificate at American University, and holds a variety of technical and professional certifications, including the Project Management Professional (PMP) and Certified Information Systems Security Professional (CISSP) certifications.

WRITTEN
TESTIMONY OF
KENNETH C. CORBIN
COMMISSIONER, WAGE AND INVESTMENT DIVISION
AND
SILVANA GINA GARZA
CHIEF INFORMATION OFFICER
INTERNAL REVENUE SERVICE
BEFORE THE
HOUSE OVERSIGHT AND GOVERNMENT REFORM COMMITTEE
ON THE FAFSA DATA RETRIEVAL TOOL
MAY 3, 2017

INTRODUCTION

Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee, thank you for the opportunity to discuss the work being done to secure the online Data Retrieval Tool (DRT) that is accessible from the fafsa.gov and StudentLoans.gov websites.

The IRS works continuously to safeguard our systems and protect taxpayer information. An important focus of this work is the ongoing battle against stolen identity refund fraud. We have made steady progress over the last few years in stopping fraudulent refund claims, criminally prosecuting those who engage in this crime, and helping minimize the adverse effect on taxpayers.

Despite all the progress we have made, the threat is constantly evolving. Fraudsters and criminal enterprises are using complex and highly sophisticated tactics to reach their target. As the IRS improves its capabilities and shuts off certain avenues of entry, identity thieves look for new ways of getting in. As the IRS enhances return processing filters and catches more fraudulent returns at the time of filing, criminals attempt to become more sophisticated at faking taxpayers' identities. We know we cannot rest and that solutions we implement are only good until the thieves find a new way to circumvent our defenses. We must stay diligent and ever watchful.

To address this challenge, the IRS is working not just to react better and faster, but to anticipate the criminals' next moves and stay ahead of them. To that end, we have used funding provided by Congress to increase our monitoring, detection, and analytical capabilities in relation to suspicious activity within our systems. These improvements have helped us slow down identity thieves, but we still need to do more. Congress helped us in this regard by approving $290 million in additional funding in 2016, which included $95 million to improve cybersecurity. We used a portion of that funding to implement the use of monitoring equipment and other capabilities that are more sophisticated than

what we had used previously. This has helped us detect suspicious activity in our various online tools and applications more quickly.

We have also undertaken a broad effort to review the authentication practices for programs where we share taxpayer information, and strengthen those practices where necessary.

One example of this effort was our decision last year to eliminate the electronic filing Personal Identification Number (e-file PIN) as an option for taxpayers to use to verify their identity when filing their tax return. Taxpayers received the e-file PIN by entering certain identifying information into an electronic tool on IRS.gov. After discovering unauthorized attempts had been made to obtain e-file PINs using data stolen from sources outside the IRS, we halted use of the e-file PIN. Although our analysis of the situation found that no personal taxpayer data was compromised or disclosed by IRS systems, we believe it was necessary to discontinue the e-file PIN to protect taxpayers and their data.

Our efforts to strengthen authentication practices also extend to programs where the IRS is authorized to share taxpayer data with organizations that use it to verify eligibility for customers who apply for loans. Since last summer, we have been working with banks, mortgage companies, and others to ensure they were implementing strong “know your customer” requirements.

Along those lines, in June 2016, the IRS announced new, stronger requirements for participants using the Income Verification Express Service (IVES). IVES is used by pre-screened companies who, in turn, are hired by mortgage firms and loan companies that need to verify applicants’ income. Going forward, the IRS will only accept requests for taxpayer data from IVES participants who certify that they are using the new requirements to verify their clients. We took this step out of an abundance of caution to protect taxpayer information as well as safeguard IVES, which has been a successful program for the government, taxpayers, and the private sector since 2006.

THE FEDERAL STUDENT AID DATA RETRIEVAL TOOL

Applying for student financial aid is another area where we are concerned about the potential for bad actors to obtain taxpayer information fraudulently. We are working with the Department of Education to secure the online process through which student financial aid applicants obtain their federal tax information, which they need to complete the *Free Application for Federal Student Aid* (FAFSA®) or apply for an income-driven repayment (IDR) plan for their student loans. The focus of our concern is the Data Retrieval Tool (DRT), which allows an applicant to automatically populate the FAFSA, or an IDR plan application, with the required information from the applicant’s tax return.

In the fall of 2016, we had an early indication of a potential misuse of the DRT to access taxpayer data. While the attempt was not successful, it highlighted the possibility that, with stolen personal information, a bad actor could pose as a student, begin completing an online application for student aid using the FAFSA, and give permission for the IRS to populate that application with tax data using the DRT.

Although the attempt failed, we immediately advised the Department of Education of our concern that criminals could access the tool and fraudulently obtain taxpayer data. We explored several potential solutions to address these concerns.

At the time, we agreed with the Department of Education that since we had no evidence of confirmed criminal activity and given that cutting off the tool could potentially increase the application burden for a large number of students and parents, we would not shut down the DRT immediately, but monitor usage, while we explored solutions that would meet both of our needs. We made this decision with the understanding that further action would be necessary if any indication of criminal activity was identified.

In early 2017, the IRS's Cybersecurity Fraud and Monitoring team observed anomalous behavior on the Federal Student Aid DRT using the IDR application. The IRS immediately increased monitoring and blocked Internet Protocol (IP) addresses based on the suspicious activity observed. The Department of Education performed additional analyses on the suspicious activity and determined that it was not fraudulent attempts to access tax data from the IRS.

Shortly thereafter, we learned of an incident that led us to determine that there was evidence of identity theft and likely fraud. Based on this incident, the IRS cybersecurity team was able to identify a pattern of suspicious activity. The pattern indicated criminals, having obtained personal information from sources outside the IRS, were masquerading as applicants for student financial aid and using the DRT to obtain enough tax return information to allow them to file fraudulent tax returns. The data obtained through the unauthorized use of the tool were later used, in some instances, in an attempt to file fraudulent returns. Having confirmed that the activity was fraudulent, we decided to turn off the DRT.

STEPS TO HELP TAXPAYERS

The IRS is working to identify the number of taxpayers affected by questionable DRT use. We are also continuing to review the extent to which this contributed to fraudulent tax returns. We have identified some instances where our strengthened fraud reviews stopped a significant number of questionable tax returns by filers who accessed the DRT.

Our investigation of unauthorized attempts to access the DRT found that approximately 100,000 individuals may have had their taxpayer information compromised. We have mailed letters to these taxpayers to alert them to the possibility of suspicious activity related to their personal information, and to offer them free credit monitoring.

Along with notifying these taxpayers, the IRS is also marking their accounts to provide additional protection against the possibility that an identity thief could file a false return using their information. We are also giving these taxpayers the opportunity to obtain an Identity Protection Personal Identification Number (IP PIN). This will further safeguard their IRS accounts and help them avoid any problems filing returns in future years.

The roughly 100,000 taxpayers identified as potentially affected by this incident includes approximately 8,000 for which a return has been filed and a refund issued. We are analyzing these returns to determine if any of them are fraudulent.

IMPROVING E-AUTHENTICATION FOR THE DRT

The original IRS authentication process set up for DRT users to verify their identities was standard at the time the DRT was developed in 2009. This required users to provide their first and last name, Social Security Number (SSN), date of birth, tax return filing status, and address of record. .

We conducted an e-authentication risk assessment, completed last fall, which indicated the need for strengthened authentication procedures. Since then, we have worked collaboratively with the Department of Education to determine how best to strengthen these procedures, both for our DRT and their online FAFSA and IDR plan applications.

In working with the Department of Education, we recommended several potential solutions. We first looked at short-term solutions, but none of the ones proposed met all of the security requirements that we identified. The longer-term solutions we explored included the following:

- Strengthening user authentication protocols to a level to prevent unauthorized users from viewing tax return data using the DRT;
- Randomizing or obscuring the AGI and other data fields in such a way that what is viewed is not an exact depiction of the applicant data to be transmitted, making it less useful to criminals;
- Masking and encrypting the information so that the applicant would not be able to view it, but could still transmit it to the Department of Education;
- Exploring a legislative change to Internal Revenue Code section 6103 that would authorize the Department of Education to receive the data directly from the IRS, which would greatly increase security.

After consulting with the Department of Education we decided that, in the absence of legislation, the most effective solution would be to mask and encrypt the data, as envisioned in the encryption solution mentioned above, so that the data would not be visible to the applicant, thereby shielding information from last year's tax return from anyone masquerading as the student applicant. Randomizing or obscuring the information would not provide sufficient protection, and increasing the authentication procedure would make the tool unavailable to most applicants.

The option we chose balances the need to protect the taxpayer data while trying to make the solution accessible to the students applying for financial aid. The IRS is working toward an operational system upgrade for the IDR application by late May or early June 2017. The encryption upgrade is also planned the for 2018–19 FAFSA launch on October 1, 2017.

In the interim, families can still complete applications for student financial aid by manually providing the requested financial information from copies of their tax returns. And, if necessary, they can obtain a copy of those returns either online through the Get Transcript application, by mail, or from their tax preparer. Although we realize this is more burdensome than using the DRT, we have a responsibility to protect the DRT and all of our online tools from identity thieves. We will continue to discuss with the Department of Education other options for long-term solutions that ensure that the FAFSA remains accessible to everyone who wants to pursue postsecondary education while protecting sensitive taxpayer data.

Chairman Chaffetz, Ranking Member Cummings and Members of the Committee, that concludes our statement. We would be happy to take your questions.

Kenneth Corbin
Internal Revenue Service
Commissioner, Wage and Investment Division

Kenneth (Ken) Corbin serves as the Commissioner of the Wage and Investment (W&I) Division, responsible for the administration of tax laws governing individual wage earners in the United States. The W&I Division delivers customer service (including telephone and face-to-face assistance) and tax return processing for all of America's taxpayers as well as compliance activities for W&I taxpayers. Ken was appointed as Commissioner, W&I Division, in January 2017.

Prior to this assignment, Ken served as Director, Return Integrity and Compliance Services in the W&I Division. He was responsible for strengthening the integrity of the tax system through pre-refund revenue protection and the oversight of refundable credits.

Ken began his career in government service in 1986. Ken holds bachelor’s degrees in chemistry and philosophy from Emory University in Atlanta, Georgia.

Gina Garza
Internal Revenue Service
Chief Information Officer

Gina Garza serves as the Chief Information Officer for IT where she is responsible for all aspects of our systems that operate the nation's tax infrastructure. She oversees the 6,800 person IT organization that maintains the 500+ systems and supports the processing of 200 million tax returns annually.

In her prior role as the Deputy Chief Information Officer for IT, Gina drove the continued transformation of the IT organization to world class while helping drive the successful implementation of multiple initiatives. She was responsible for overseeing day-to-day operations of the organization and providing strategic and operational oversight for many functions within IT.

Prior to becoming the DCIO, Gina served as the Associate Chief Information Officer (ACIO) for the Affordable Care Act Program (ACA) Management Office. In her role, she stood up the ACA program office, developed the strategy, plan and implemented the initial release of ACA. Prior to serving as ACIO for ACA, Gina established a program management capability for a multi-billion-dollar modernization program. She was also part of a core team of executives that developed the "IRS Modernization Blueprint and Business Case" that defined the roadmap for transforming the IRS's information systems.

HEARING BEFORE THE
OVERSIGHT AND GOVERNMENT REFORM COMMITTEE
U.S. HOUSE OF REPRESENTATIVES

"Reviewing the FAFSA Data Breach"

Testimony of
Timothy P. Camus
Deputy Inspector General for Investigations
Treasury Inspector General for Tax Administration

May 3, 2017

Washington, D.C.

TESTIMONY
OF
TIMOTHY P. CAMUS
DEPUTY INSPECTOR GENERAL FOR INVESTIGATIONS
TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION
before the
OVERSIGHT AND GOVERNMENT REFORM COMMITTEE
U.S. HOUSE OF REPRESENTATIVES

"Reviewing the FAFSA Data Breach"

May 3, 2017

Chairman Chaffetz, Ranking Member Cummings, and Members of the committee, thank you for the opportunity to testify about the 2017 criminal exploitation of the Free Application for Federal Student Aid (FAFSA) and Data Retrieval Tool (DRT).

The Treasury Inspector General for Tax Administration (TIGTA) was created by Congress in 1998 to help maintain the 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's Office of Investigations investigates allegations of IRS employee criminal and administrative misconduct, attempts to threaten or harm IRS employees, facilities or IRS data infrastructure, and external attempts to corrupt tax administration through the impersonation of IRS employees and programs, taxpayer data exploitation, and attempts to bribe IRS employees.

For the purposes of this hearing, my testimony will focus on the protection of taxpayer information, specifically the 2017 exploitation of the FAFSA application and the DRT.

---

[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*.

RECENT CHALLENGES IN SECURING TAXPAYER DATA

As cybersecurity threats against the Federal Government continue to grow, protecting the confidentiality of taxpayer information will continue to be a top concern for the IRS and for TIGTA. According to the Department of Homeland Security's U.S. Computer Emergency Readiness Team, Federal agencies reported 77,183 cyberattacks in FY 2015, an increase of approximately 10 percent from FY 2014. The increasing number of data breaches in the private and public sectors means more personally identifying information than ever before is available to unscrupulous individuals.

Due to the $400 billion dollars the IRS issues in refunds and the 242 million tax returns it processes each year that contain extremely valuable information for identity thieves, the IRS has become a favorite target of cyber criminals located all over the world. For example, in May 2015, criminals launched a coordinated attack on the IRS e-Authentication portal that resulted in the exploitation of the IRS Get Transcript Application, as well as the IRS IP PIN application. It is estimated that more than 110,000 taxpayers were impacted by this attack.

A subsequent review of all of the activity on the system revealed that more than 700,000 taxpayers were impacted by similar abuses of the system by multiple bad actors over an extended period of time. In January 2016, a coordinated effort was launched that exploited the IRS Electronic Filing PIN (e-File PIN) tool. The e-File PIN tool was created to provide taxpayers with a special PIN number that would allow the taxpayer to electronically file a Federal tax return. The IRS estimates the exploitation resulted in the issuance of over 100,000 e-File PINs that were used to file over $100 million dollars of fraudulent tax returns. As a result of this exploitation, on June 23, 2016, the IRS announced that it had disabled the e-File PIN application. Numerous investigations are underway on the individuals who obtained taxpayer information from both of these attacks.

FAFSA AND THE DRT

The DRT allows students and parents to access their adjusted gross income (AGI) information through an interface with the IRS to complete the FAFSA by transferring the AGI information directly into their FAFSA application form. FAFSA on the web was first introduced in on June 30, 1997 and the IRS DRT component of the process was activated on January 28, 2010.

Following the e-Authentication Get Transcript exploitation in May 2015, the IRS reevaluated the authentication risk on outward-facing online applications based on today's known cyber-crime environment. The IRS conducted this e-Authentication Risk Assessment (eRA) on 45 applications, including the FAFSA and DRT process. On October 25, 2016, the IRS determined the risk factors involving financial loss or agency liability, harm to agency programs or public interests, and the risk of unauthorized release of sensitive information utilizing the FAFSA and the DRT were all scored in the low risk category. On December 5, 2016, the Risk Assessment Form and Tool was signed by the IRS, and the FAFSA and DRT remained operational.

It appears that identity thieves used personal information of individuals that they obtained outside the tax system to start the FAFSA application process in order to secure the AGI tax information through the DRT. The IRS' current estimate for the number of impacted taxpayers is approximately 100,000. TIGTA is conducting a joint investigation of this exploitation with IRS Criminal Investigation and the Department of Education Office Inspector General (Education OIG). As part of our investigation, we are also looking back to see if there was an earlier bulk exploitation of the FAFSA and the DRT process. TIGTA is also planning to initiate an audit to review this issue.

In September 2016, TIGTA detected an attempted access to the AGI of a prominent individual. When we investigated the attempted access, we determined that the FAFSA application and the DRT were used in this attempt. Since FAFSA is a Department of Education application, we notified the Education OIG and we notified the IRS Privacy, Governmental Liaison and Disclosure (PGLD) program office. We initiated a joint investigation with the Education OIG that included the Cyber Crimes Task Force. The investigation identified the individual responsible for the attempted access and he was arrested. This case is still proceeding through the court system. In November 2016, we noticed another attempted access of the same prominent individual's AGI through the FAFSA and the DRT, this time, from an entirely different location. We have included this attempted access in our investigation activity and we also notified the PGLD program office. This activity is still under investigation.

On January 25, 2017, the IRS reported to us that a high number of Taxpayer Identification Numbers were being processed through FAFSA and the DRT. The IRS told us that when they shared this observation with the Department of Education, Education told the IRS that they believed the activity was related to student loan consolidation activity.

On February 27, 2017, a complainant reported that he received a copy of his tax transcripts at his home with a letter telling him that he had requested them. The complainant reported he never ordered a copy of his tax transcripts. When his tax account information was researched, we learned that the complainant's AGI had been accessed through the FAFSA and the DRT process. As a result, we determined that the January activity that the IRS observed was proof that an exploitation was under way. Initial analysis showed there were 8,000 questionable accesses at that time.

On March 3, 2017, the IRS reported that they disabled the DRT due to privacy concerns and to protect sensitive taxpayer data.

We are continuing our criminal investigations of this activity and are reviewing evidence and information obtained from the investigations of the prior e-Authentication exploitations to determine if the FAFSA and DRT criminal activity was launched by the same individuals and groups. In one instance, we found evidence that as far back as February 2016, the subject of an e-Authentication investigation discussed the availability of AGI information using FAFSA and the DRT. After comparing additional log file information and email addresses, we now have very good indications that in some instances, the same individuals and groups engaged in criminal activity on the e-Authentication portal are involved in this exploitation of the FAFSA and the DRT.

We at TIGTA take seriously our mandate to provide investigative coverage of issues that confront the IRS in its administration of our Nation's tax system. As such, as we conduct our investigations of the criminals who are responsible for the cyber exploitations, we share the information we find with the IRS in order to help protect the IRS' data infrastructure. We plan to provide continuing coverage of the IRS' efforts to operate free from criminal activity in the electronic environment.

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

Timothy P. Camus
Deputy Inspector General for Investigations

Mr. Timothy P. Camus has served in the Treasury Inspector General for Tax Administration (TIGTA) and the Internal Revenue Service Inspection Service, TIGTA's predecessor organization, as a Special Agent, for over 25 years.

After an exemplary investigative career, Mr. Camus was promoted into TIGTA management. In June 2003, Mr. Camus became a member of the Senior Executive Service, and in January 2011 he was promoted to the position of the Deputy Inspector General for Investigations for TIGTA. As the Deputy Inspector General for Investigations, Mr. Camus is responsible for overseeing and leading all aspects of TIGTA's law enforcement mission.

During his law enforcement career, Mr. Camus has successfully investigated domestic terrorism, death threats made against public officials, bribery and extortion cases, as well as thefts of Government property and all other facets of white collar crime and fraud that impact the IRS. In 2008, Mr. Camus was awarded the Presidential Rank Award for Meritorious Service.