Electronic Tax Administration Advisory Committee

ANNUAL REPORT TO CONGRESS

June 2020

Publication 3415 (Rev. 6-2020) Catalog Number 28110R Department of the Treasury **Internal Revenue Service** www.irs.gov

IRS ELECTRONIC TAX ADMINISTRATION ADVISORY COMMITTEE

The Chair would like to recognize the below ETAAC members, who spent thousands of volunteer hours researching recommendations and developing this Report.

Luanne Brown

Latryna Carlton

Daniel Eubanks

Larry Gray

Jenine Hallings

Michael Jackman

John Kreger

Suzanne Kruger

Laura Macca

Julie Magee

Ada Navarro

Kathy Pickering

Phillip L. Poirier, Jr. (Chair)

Lynnette T. Riley

Cynthia Rowley

Gene Salo (Vice Chair)

John Sapp

Joseph Sica

Mark Steber

Matthew Vickers

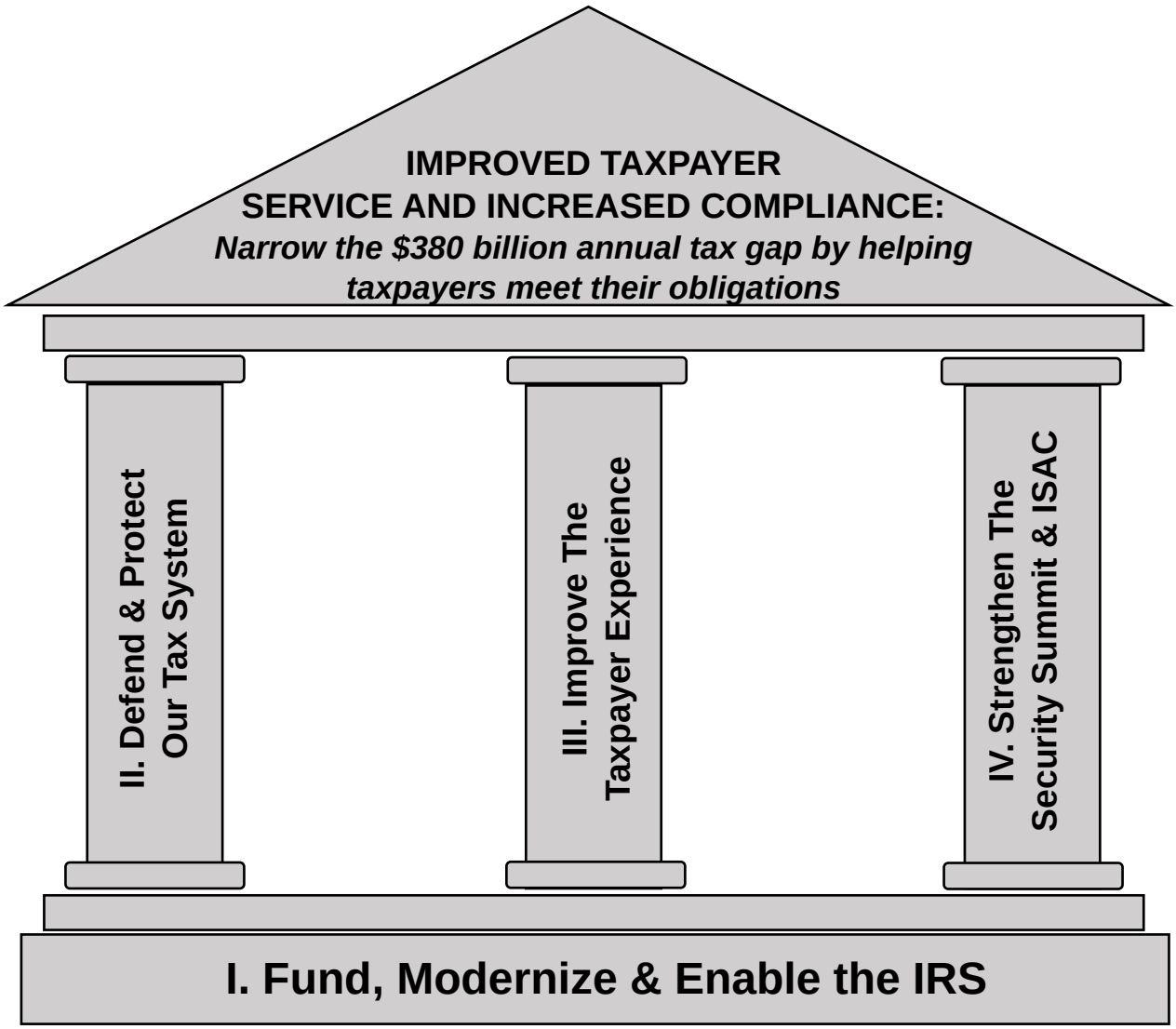
The ETAAC would like to recognize the IRS employees and leadership who supported the development of this Report. The ETAAC appreciates their responsiveness and candor in answering our questions and providing information. Our nation is fortunate to have their continued expertise and commitment.

ETAAC would like to specially recognize members who are completing their terms:

- 3 Years: Michael Jackman, Suzanne Kruger & Ada Navarro
- 4 Years: Kathy Pickering, Phillip Poirier, John Sapp, Joseph Sica & Mark Steber

A background on ETAAC can be found in Appendix A. ETAAC member biographies can be found in Appendix B. *(6/9/20)*

INTRODUCTION



This Report is organized to provide key insights at a glance or, alternatively, deeper insights and analysis.

For a ***high-level overview***, review the following Executive Summary and the Summary List of ETAAC 2020 Recommendations. To gain a ***deeper context*** for our 2020 recommendations, review the Current Environment for Electronic Tax Administration, About the IRS Security Summit and the Detailed Support for ETAAC 2020 Recommendations sections that follow the Table of Contents.

Finally, review the entire Report to get the fullest context and analysis.

EXECUTIVE SUMMARY

The Electronic Tax Administration Advisory Committee (ETAAC) is pleased to deliver its 2020 Annual Report to Congress.

The Security Summit continues to make strong progress in fighting IDTTRF

Consistent with its charter, ETAAC's primary focus continues to be on the fight against Identity Theft Tax Refund Fraud (IDTTRF)[1], improving cybersecurity and enabling electronic tax administration while protecting taxpayer information.

IDTTRF continues to threaten the integrity of our voluntary compliance tax system at both the federal and state levels. The wholesale theft of huge volumes of personal information has provided criminals and other bad actors with detailed and accurate taxpayer information. Our sophisticated adversaries can use this information to create and file returns that look nearly identical to those of the legitimate taxpayer. It would be great if there were a silver bullet to make it easy for the IRS to spot these fraudulent returns among the hundreds of millions of legitimate returns. Unfortunately, there is no silver bullet.

To protect our tax system, the Security Summit must continue to drive a unified and collaborative approach among all of the stakeholders.[2] Fortunately, the IRS, states and private industry have made substantial funding and personnel commitments to the Security Summit and ISAC.[3] Ongoing funding and investment in programs, technology and staff will be critical to the continued maturation, evolution and success of the Security Summit and ISAC.

Most importantly, ETAAC would like to recognize the Security Summit's continuing progress under the IRS's leadership and with the significant support and commitment of states and industry. The Security Summit is a living demonstration of the benefits of taking on common challenges with a unified and collaborative public/private approach.

The fact that ETAAC has recommendations for improvement does not, in any way, diminish the remarkable accomplishments of the IRS, states and industry in this area.

The response to the COVID-19 pandemic proves the resilience of our tax system

The coronavirus pandemic is having devastating effects on our nation. In the face of the pandemic challenge, policymakers again turned to the IRS, which worked with states and the broader tax industry to inform citizens and deliver relief in the form of economic impact payments.

In the first three weeks of the program alone, the IRS was able to deliver nearly 90 million payments worth nearly $160 billion and delivered more than 150 million payments by the end of May.[4] This is a remarkable achievement, which included not

[1] IDTTRF is sometimes referred to as Stolen Identity Tax Refund Fraud (SIRF).

[2] The About the IRS Security Summit section of this Report reviews the key accomplishments and current focus/priorities of the Security Summit and ISAC.

[3] "ISAC" refers to the IDTTRF Information Sharing and Analysis Center, which is further described in the About the Security Summit section of this Report.

[4] See IRS News Release IR-2020-80, April 24, 2020 (https://www.irs.gov/newsroom/treasury-irs-deliver-89-point-5-million-economic-impact-payments-in-first-three-weeks-release-state-by-state-economic-impact-payment-figures).

only delivering payments but also developing associated regulations and procedures and answering a myriad of questions from taxpayers and small businesses.

The IRS was facing key challenges even before the COVID-19 pandemic

At the outset, the current environment is driving some key observations for ETAAC:

1. The fiscal condition of the federal government is under tremendous strain – the IRS must narrow the $380 billion annual tax gap.
2. Modernization of the IRS is an essential component of narrowing the tax gap. Modern technologies play a fundamental role in the IRS's ability to improve taxpayer services, deliver a 21st Century taxpayer experience, collect revenues owed to the government and increase the IRS's operating effectiveness and efficiency.
3. Full funding of the IRS's FY2021 budget request, including its request for a Program Integrity Cap Adjustment,[5] is foundational to IRS enforcement and modernization.
4. Cybercriminals continue to attempt to steal billions of dollars in refunds and are constantly probing for new vulnerabilities – the IRS and the Security Summit cannot let down their guard.
5. Beyond IDTTRF, our tax system is exposed to disruption by adversaries intent on interrupting the flow of tax revenues, refunds and other payment streams critical to our nation and economy.

The pandemic, and the nation's response to it, only reinforces the need to enable IRS modernization to deliver 21st Century taxpayer experiences and enhance its enforcement efforts, both of which are critical to closing the tax gap.

ETAAC's 2020 recommendations are intended to address our key observations

Our recommendations are framed around the four themes that build on each other. Most importantly, our first set of recommendations focus on Congressional action to enable the IRS to better serve this nation and its taxpayers.[6] Then, our remaining recommendations focus on improving cybersecurity, improving taxpayer services and fighting IDTTRF.[7]

At a summary level, our Report's four themes and underlying recommendations are:

Theme #1: Fund, Modernize and Enable the IRS

- Fully fund the IRS Fiscal Year (FY) 2021 budget request

[5] Federal budgeting statutes permit "cap adjustments" under particular circumstances to increase spending for specified purposes without triggering a breach of statutory spending limits. In addition to its FY2021 base appropriations, the IRS has proposed a Program Integrity Cap (PIC) Adjustment to fund investments to expand and improve the IRS's overall tax enforcement program.

[6] See Recommendations #1 - #4 (and Supporting Analysis) in Part I of Detailed Support for ETAAC 2020 Issues & Recommendations.

[7] See Recommendations #5 - #16 (and Supporting Analysis) in Parts II, III and VI of Detailed Support for ETAAC 2020 Issues & Recommendations.

- Consider and approve the IRS's request for an FY2021 Program Integrity Cap Adjustment
- Monitor and enable government-wide digital identity policies and initiatives
- Provide IRS with the authority and necessary funding to enforce security standards

Theme #2: Defend and Protect our Tax System

- Collaborate on the identification and mitigation of disruption threats to our tax system
- Engage with the FTC to assess impact and implementation of proposed changes to FTC Safeguards Rule
- Study information security practices and identify vulnerabilities in the tax preparer community

Theme #3: Improve the Taxpayer Experience

- Collaborate on the identification and piloting of promising digital identity solutions
- Implement taxpayer-controlled "real-time" protections
- Expand collaboration on the design and launch of the IRS 1099 internet-based service
- Increase accuracy of EIN responsible party information

Theme #4: Strengthen the Security Summit and ISAC

- Evaluate the Taxpayer First Act's (TFA) impact on the Security Summit and sustain the energy and commitment of Security Summit and ISAC participants
- Collaborate with state and industry ISAC participants to implement TFA's ISAC-related provisions
- Implement a more structured onboarding process to mitigate the adverse impact of continuing ISAC turnover
- Provide a more structured training program to improve ISAC participant performance
- Implement real-time EFIN and PTIN validation capabilities

Closing Thoughts

Although ETAAC is not suggesting any silver lining, the impact of and response to the pandemic provides a time to capture some critical lessons learned. ETAAC encourages the IRS, states and the tax industry to take this opportunity to capture any lessons learned from the pandemic response: What worked well and what can be done better? What are the underlying causes of any deficiencies, and what can be done about them? Does IRS need more established "incident response" teams and procedures to facilitate discussions, feedback and communications with state, industry and taxpayer stakeholders?

A lessons learned exercise would also be a good time to review the IRS Security Summit's structure and operations and identify specific opportunities to drive and sustain its effectiveness, efficiency and participant energy and commitment.[8]

Finally, ETAAC would like to recognize the IRS's employees and leadership for their continued efforts to administer an increasingly complex tax system, meet taxpayer service expectations, improve cybersecurity, fight IDTTRF and successfully process billions of transactions and hundreds of millions of tax returns every year. The United States tax system could not operate without their dedication, commitment, and talent. IRS employees and managers have made themselves available during the filing season and on other occasions to brief ETAAC on a variety of issues. ETAAC is most grateful for their thoughtful and candid insights essential to the preparation of this Report.

Respectfully submitted,

Phillip L. Poirier, Jr.	Gene Salo
ETAAC Chair	ETAAC Vice Chair

[8] See ETAAC Recommendation #12.

SUMMARY LIST OF ETAAC 2020 RECOMMENDATIONS

Below are ETAAC's 2020 recommendations organized around the Report's four themes. Our detailed analysis and explanation of each recommendation is found in the "Detailed Support for ETAAC 2020 Recommendations" section of this Report.

I: FUND, MODERNIZE & ENABLE THE IRS

RECOMMENDATION #1: *Fully fund the IRS FY2021 budget request*

Congress should fully fund the IRS's FY2021 budget request to enable the IRS to deliver 21st Century taxpayer experiences, narrow the $380 billion Tax Gap to meet the nation's pressing fiscal needs, protect the tax system and build a modern information system infrastructure. Any appropriations should be allocated across the IRS's four appropriations accounts in a manner to enable the achievement of its stated taxpayer service, enforcement and modernization goals.[9]

RECOMMENDATION #2: *Consider and approve the IRS's request for an FY2021 Program Integrity Cap Adjustment*

Congress should amend Title 2 U.S. Code § 901 to add the IRS Program Integrity Cap Adjustment to isolate this tax revenue generating opportunity from competing priorities within the Financial Services and General Government appropriations' funding cap. This action will provide a foundational investment for a multi-year effort to restore IRS enforcement levels, increase revenue to the Treasury and strengthen the nation's tax system.

RECOMMENDATION #3: *Monitor and enable government-wide digital identity policies and initiatives*

Congress should monitor the direction and progress of government-wide digital identity policies and initiatives, and provide legislative and funding support as necessary.

RECOMMENDATION #4: *Provide IRS with the authority and necessary funding to enforce security standards*

Congress should grant the IRS the clear legal authority and provide the associated funding to issue and enforce appropriate information security standards and guidance in the area of tax administration, which could include adopting existing or establishing new administrative, technical and physical safeguards, implementing required education and training, and providing ongoing guidance.

[9] The IRS's four appropriations accounts are: Taxpayer Services, Enforcement, Operations Support and Business Systems Modernization.

II. DEFEND & PROTECT OUR TAX SYSTEM

RECOMMENDATION #5: *Collaborate on the identification and mitigation of disruption threats to our tax system*

The IRS should work with the Security Summit to evaluate and develop responses to potential attacks by adversaries intended to disrupt our tax system and, thereby, interrupt the flow of government revenues and tax refunds.

RECOMMENDATION #6: *Engage with the FTC to assess impact and implementation of proposed changes to FTC Safeguards Rule*

The IRS should work with the FTC and tax preparation community (including VITA/TCE) to understand the substance and impact of the FTC's proposed amendments to the FTC Safeguards Rule, and implement a plan to educate and enable the tax preparation community to comply with any new security requirements without the significant and unnecessary disruption of this community's ability to serve taxpayers.

RECOMMENDATION #7: *Study information security practices and vulnerabilities in the tax preparer community*

As further outlined by ETAAC in this Report, the IRS should engage a qualified third party to conduct an initial study of the tax preparer community to understand its different segments and operating models, determine the state of its information security practices and vulnerabilities, and identify the range of high level strategic options and associated costs to remediate these risks.

III. IMPROVE THE TAXPAYER EXPERIENCE

RECOMMENDATION #8: *Collaborate on the identification and piloting of promising digital identity solutions*

The IRS should engage regularly with external subject matter experts, including Security Summit members, to identify and potentially pilot promising technologies or approaches to verify identities.

RECOMMENDATION #9: *Implement taxpayer-controlled "real-time" protections*

The IRS should continue to investigate, develop and implement proactive notification, lock/unlock and other taxpayer-controlled "real-time" protective features for individual and business taxpayer accounts.

RECOMMENDATION #10: *Expand collaboration on the design and launch of the IRS 1099 internet-based service*

The IRS should expand its existing collaboration with states and industry in the design and implementation of the TFA-mandated 1099 service in a way that anticipates its integration into future modernized IRS systems.

RECOMMENDATION #11: *Increase accuracy of EIN responsible party information*

The IRS should review current EIN-related processes with Security Summit and other external stakeholders to obtain recommendations to increase awareness of and compliance with the EIN holder's obligation to report changes in its responsible party.

IV. STRENGTHEN THE SECURITY SUMMIT & ISAC

RECOMMENDATION #12: ***Evaluate TFA impact on Security Summit and sustain energy and commitment of participants***

The IRS should work with the Security Summit's state and industry leadership to evaluate the impact of any IRS organizational redesign pursuant to the Taxpayer First Act on the Security Summit's structure and operations, and to identify and act on specific opportunities to drive and sustain the Summit's effectiveness, efficiency and participant energy and commitment.

RECOMMENDATION #13: ***Collaborate with State and Industry ISAC participants to implement TFA's ISAC-related provisions***

The IRS should collaborate with states and industry to develop and implement Section 2003 (b) and (c) of the Taxpayer First Act regarding ISAC performance metrics, information sharing agreements and related policies and procedures.

RECOMMENDATION #14: ***Implement a structured on-boarding process to mitigate the adverse impact of continuing ISAC turnover***

The IRS should enable the ISAC Trusted Third Party to develop an on-boarding process including a review of ISAC reference and operational materials to mitigate the adverse impact of IRS, state and industry personnel turnover and accelerate the value provided by and to new ISAC participants.

RECOMMENDATION #15: ***Implement a more structured training program to improve ISAC participant performance***

The IRS should enable the ISAC Trusted Third Party to implement a more structured approach for the development and delivery of ISAC platform training.

RECOMMENDATION #16: ***Implement real-time EFIN and PTIN validation capabilities***

The IRS should continue to develop and implement a system to enable real-time electronic EFIN validation by authorized third parties and, once launched and operating effectively, evaluate options to extend this functionality to real-time electronic PTIN validation.

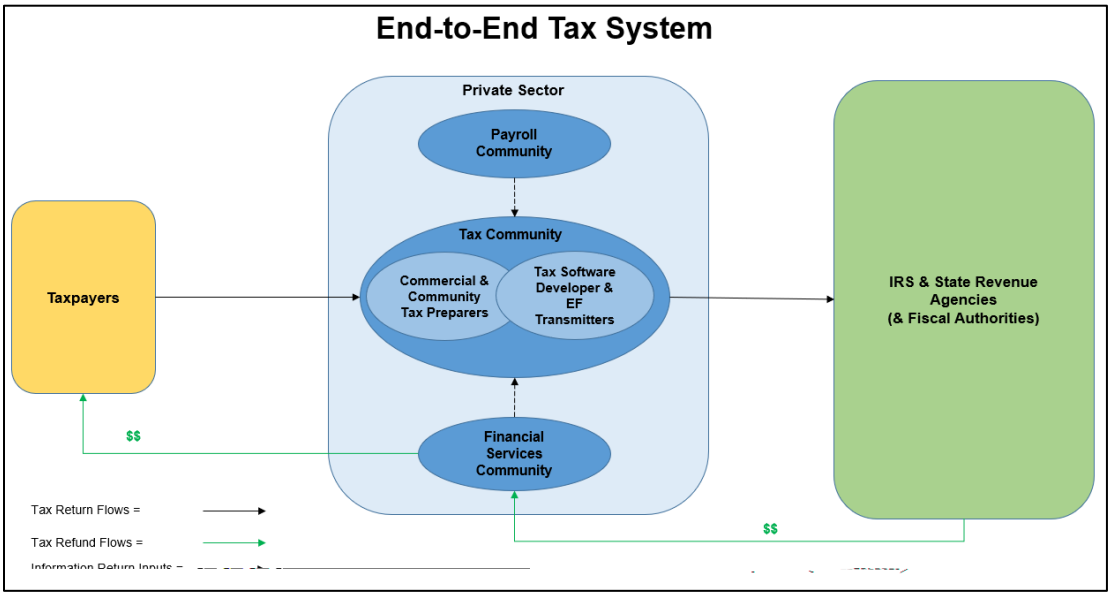
TABLE OF CONTENTS

CURRENT ENVIRONMENT FOR ELECTRONIC TAX ADMINISTRATION

The U.S. has a highly integrated government/private sector tax system

The federal and state tax laws consist of a broad set of statutes, regulations, rules, procedures, forms and publications. In totality, their volume and complexity can easily overwhelm the average taxpayer.

As a consequence, the tax administration system that serves those taxpayers has necessarily evolved into a highly integrated electronic system developed and operated by both the government and private sectors. The tax system's stakeholder communities are as varied as the U.S. population and its economy, and include the IRS, state revenue agencies, tax professionals, VITA programs, tax preparation and payroll service companies, technology companies, financial services companies and, of course, taxpayers.



The tax system is critical to the U.S. government, economy and taxpayers

The IRS is responsible for administering the nation's tax system. In this capacity, the IRS must both help taxpayers understand their tax responsibilities and enforce the law with integrity and fairness.

At the macroeconomic level, our tax system has a huge impact on the government and economy. During the 2019 filing season, the IRS collected over $3.6 trillion in gross taxes, processed approximately 255 million federal tax returns and forms, and issued over $300 billion in income tax refunds.[10] To put these measures in perspective, the IRS generated 95 percent of the funding that supports the federal government's operations.

Federal tax refunds have a profound impact on individual taxpayers. In 2019, about 110 million families and individuals received an average refund of approximately $2,800 – ninety percent of which were issued within 21 days of filing. Any disruption in refund

[10] IRS Congressional Budget Justification & Annual Performance Report and Plan, Fiscal Year 2021, p. IRS-2 (FY21 IRS Congressional Justification) (See https://home.treasury.gov/system/files/266/02.-IRS-FY-2021-CJ.pdf).

issuance puts pressure on American taxpayers, many of whom live paycheck-to-paycheck and struggle to pay unexpected expenses such as a car repair or broken refrigerator because of the lack of savings or access to affordable credit.

Every tax filing season presents its unique challenges

2019 filing season's challenges were significant

It is a challenge to operate the tax system in a "normal" year. But, by any measure, the 2019 filing season was anything but normal.

The federal government shutdown on December 22, 2018 and did not reopen until January 25, 2019. This 35-day period was the longest U.S. government shutdown in our country's history. Despite this disruption, the IRS completed the filing season and even processed approximately 15 million returns on the last day of the primary filing season – a testament to the IRS's readiness and resilience in a fast moving digital world where taxpayers have increasing expectations for responsive service delivery up until the last moment.

2020 filing season's challenges have been unprecedented

The challenges of the 2020 filing season have been unprecedented. In the throes of the COVID-19 global pandemic, many would look back almost fondly on the challenges presented by the 2019 filing season.

Our nation's economy was significantly impacted and the IRS had to deal with changes in tax filing deadlines and make other accommodations to reduce financial pressure on American taxpayers.

On top of the filing season, U.S. policymakers again relied on the IRS to find ways to deliver financial relief to taxpayers. Fortunately, the capabilities and resilience of our tax system has been demonstrated by the strong collaboration between the public and private sectors to create and implement systems, processes and procedures to register taxpayers for economic impact payments and ultimately deliver billions of dollars in financial relief.

IRS faces other continuing challenges and risks beyond filing season challenges

Each year, the Treasury Inspector General for Tax Administration (TIGTA) evaluates IRS programs, operations, and management functions to identify the areas of highest vulnerability to the nation's tax system. [11]

For FY2020, TIGTA identified the following as the IRS's top five management and performance challenges:

- Security over taxpayer data and protection of IRS resources
- Implementing tax law changes
- Addressing emerging threats to tax administration
- Supporting an enhanced taxpayer experience

[11] TIGTA Management and Performance Challenges Facing the Internal Revenue Service for Fiscal Year 2020 (October 2019) (See https://www.treasury.gov/tigta/management/management_fy2020.pdf).

- Modernizing IRS operations

ETAAC's assessment of IRS's challenges is consistent with TIGTA's

From its perspective, ETAAC is focused on six key challenges facing the IRS:

#1: Collection of tax monies owed to the federal government

#2: Adequate funding

#3: IRS systems modernization

#4: Cybersecurity of tax system

#5: IDDTRF prevention in both individual and business tax areas

#6: Protection of the tax system from operational disruption

Our recommendations are intended to address these challenges, but achieving success in each of these areas is significantly affected by Congressional appropriations.

#1: Collection of tax monies owed to the federal government

Given the nation's pressing financial demands, the IRS needs to narrow the net tax gap, which is estimated to be $380 billion per year.[12] Importantly, relatively small improvements can deliver big results in terms of federal revenues. For example, a one percent improvement in the voluntary compliance rate, currently estimated at 83.6%,[13] equals about $30 billion a year in federal net revenue.

At the highest level, the IRS needs to do three things: (i) make it easier for taxpayers to comply by providing better taxpayer service and experiences, (ii) collect taxes that are owed but not paid by improving IRS enforcement and collections, and (iii) reduce operating expenses.[14]

There is a clear opportunity to modernize the IRS, enhance taxpayer services and collect more tax revenue.

#2: Adequate funding

As further described in this Report, the IRS's workload and responsibilities have increased as the taxpayer population and tax complexity have increased over the past ten years.

During this same time period, however, IRS funding decreased an estimated 20% in real dollars,[15] which resulted in declining resources in a time of increasing demand. A simple way to depict this trend is to compare return growth with IRS fulltime equivalent headcount (FTE).

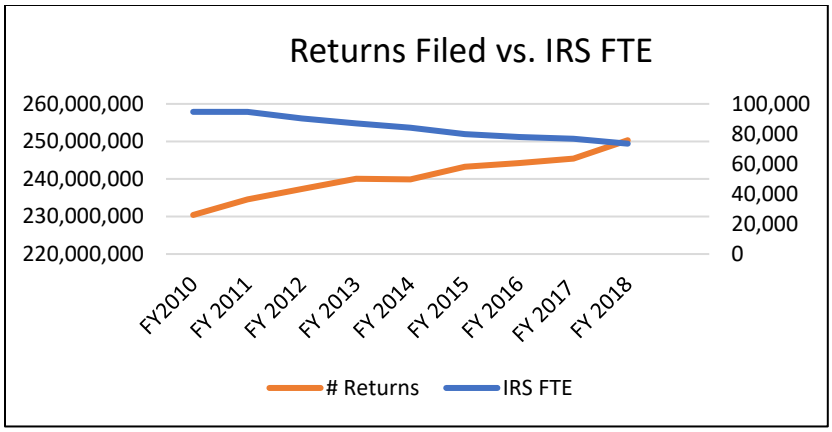
---

[12] FY21 IRS Congressional Justification, p. IRS-2.

[13] IRS Progress Update Fiscal Year 2019, p. 19 (See https://www.irs.gov/pub/irs-pdf/p5382.pdf).

[14] To narrow the Tax Gap, former Treasury Secretary Larry Summers recently recommended focusing on three areas: increasing examinations/enforcement, increasing information reporting, and improving information technology and analytics. NBER Working Paper: "Shrinking The Tax Gap: Approaches And Revenue Potential," Summers and Sarin, Nov. 2019 (See https://www.taxnotes.com/special-reports/compliance/shrinking-tax-gap-approaches-and-revenue-potential/2019/11/15/2b47g).

[15] Calculation based on IRS appropriation levels and OMB deflator tables.



Operational efficiencies alone could not fully compensate for the effect of sizeable staffing reductions on service level and quality, and the IRS was required to make considerable tradeoffs.

As a result, nearly every IRS taxpayer service and enforcement statistic has declined, reflecting a clear correlation of the amount of resources and performance.[16] For example, between FY2015 and FY2019, the IRS's Examination Coverage (i.e., audit rates) for Individuals declined from 0.8% to 0.45% and for Businesses (over $10 million in assets) from 3.9% to 1.6% -- decreases in the range of 40-60%. The bottom line is that funding reductions reduce taxpayer support and enforcement, which decreases tax revenues.

Fortunately, with Congressional support, the IRS was able to stop its staffing decline in FY2019. It has made significant progress in its hiring efforts, and expects to make approximately 7,000 external hires by the end of FY2020. Additionally, dedicated investments over the last year have helped the IRS to reduce its aged hardware infrastructure to 31% in FY2019, which was an overall reduction of 14.5% from the prior year.

#3: IRS systems modernization

The IRS has a clear plan and a sound approach to modernize its systems and operations. The IRS Integrated Modernization Business Plan[17] (Modernization Plan) will deliver improved taxpayer services and better experiences, build a foundation for enhanced revenue collection for the nation's tax system and stabilize growing operations and maintenance (O&M) costs.

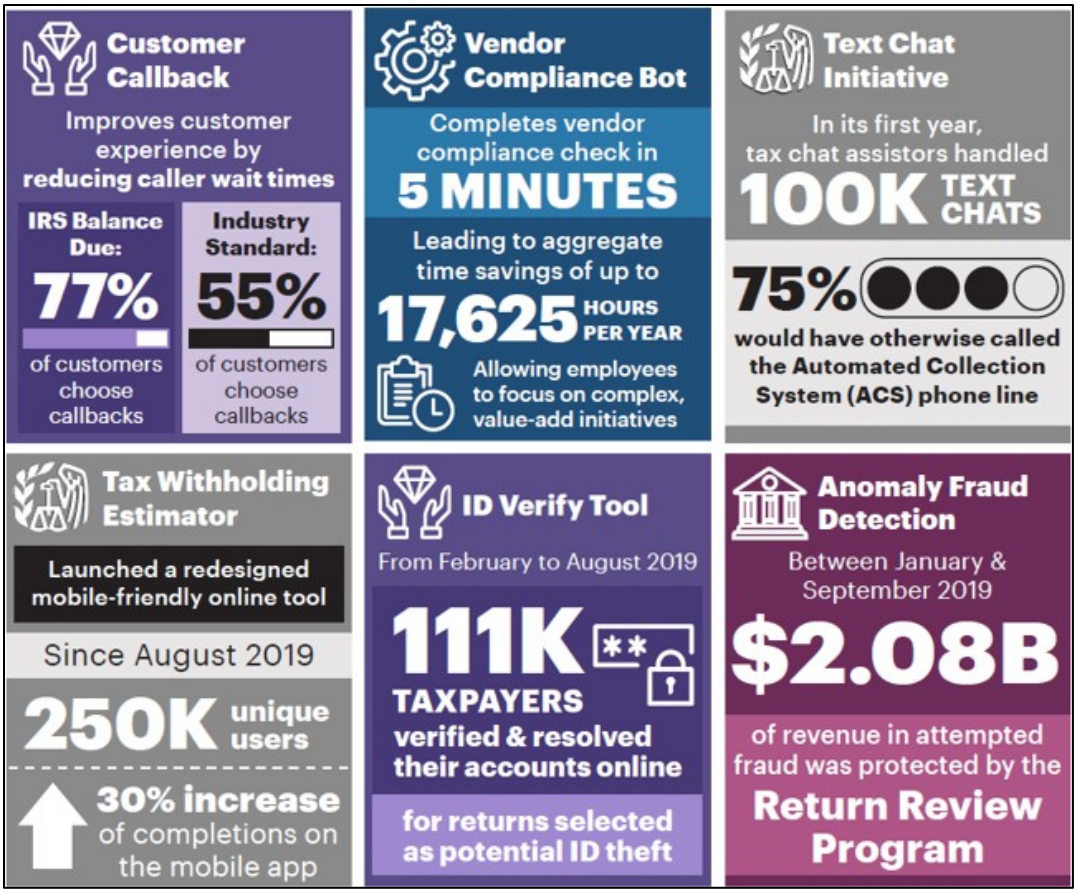
The Modernization Plan includes specific programs and initiatives focused in four key areas: Taxpayer Experience; Core Taxpayer Services & Enforcement; Modernized IRS Operations; and, Cybersecurity & Data Protection.

The first year of the IRS Modernization Plan has already delivered a positive impact on taxpayers across each modernization pillar (see below illustration). And, the IRS has made strong commitments for FY2020 deliverables and outcomes (See Appendix C).[18]

[16] FY21 IRS Congressional Justification, e.g., p. IRS-114.

[17] See https://www.irs.gov/pub/irs-utl/irs_2019_integrated_modernization_business_plan.pdf.

[18] See IRS Integrated Modernization Business Plan, FY2019 Key Insights Report (Feb. 2020).



To be successful, the Modernization Plan requires adequate Congressional funding.

#4: Cybersecurity of tax system

Cybercrime continues to increase. Between 2014-2018, the FBI's Internet Crime Complaint Center (IC3) received a total of 1,509,679 complaints accounting for an estimated $7.45 Billion in losses.[19] IC3's most recent data reflected a 16% increase in complaints and a 90% increase in associated losses.

ETAAC has previously noted the loss of sensitive information for hundreds of millions of Americans from government and private sector breaches.[20] Stolen information can enable a number of criminal activities. In the tax area, that information can be coupled with other publicly available information to be the fuel to create and file IDTTRF tax returns. In response to efforts to protect our tax system, these criminals adjust their tactics to pursue other system and stakeholder vulnerabilities. Their targets are both large and small enterprises, including the hundreds of thousands of tax professionals

[19] IC3 2018 Internet Crime Report (See https://pdf.ic3.gov/2018_IC3Report.pdf).

[20] ETAAC 2019 Annual Report to Congress, p. 5.

serving taxpayers[21] as well as service providers in the business, payroll and employment tax areas.[22]

#5: IDDTRF prevention in both individual and business tax areas

Identity Theft Tax Refund Fraud (IDDTRF) has been the principal manifestation of cybercrime in the tax system. Fortunately, the efforts of the IRS, states and private sector through the IRS Security Summit have significantly reduced IDTTRF in the individual tax system.

The IRS has developed a comprehensive, multi-faceted IDTTRF strategy. Part of this strategy includes investing in improved IDTTRF detection systems.[23] For example, the IRS's current IDTTRF detection protocols use a sophisticated risk scoring system that relies on identity theft (IDT) models and various IDT fraud indicators (sometimes called fraud filters) to identify suspicious returns. The IRS has steadily increased the number of IDT fraud filters over the past several years, which now number almost 200.[24]

The IRS also formed the Security Summit, which is described in the About the IRS Security Summit section of this Report.

Not surprisingly, cybercriminals continue to look for other financial opportunities in the tax ecosystem.

As a result, the IRS is seeing increases in IDTTRF-related activities in the areas of business tax schemes[25] and the theft of sensitive personal and tax return information from tax preparers, businesses, human resources departments and others.[26] A recent GAO Report provides a good overview of some of the challenges in this area including an overview of some commonly used schemes and high false positive rates. One specific concern is the larger average refund size associated with business return fraud.[27]

#6: Protection of tax system from operational disruption

Cybercriminals are only one threat to our tax system. There have also been allegations of nation state involvement in cyberattacks. For example, the Chinese have been accused of two of the biggest breaches in our nation's history – 21 million people in the

---

[21] The IRS's 2018 summertime security awareness campaign reported that "[d]ata thefts at tax professionals' offices continue to rise and result in fraudulent tax returns that can be especially difficult for the IRS and states to detect.").

[22] The IRS recently warned tax professionals of an uptick in phishing emails targeting them that involve payroll direct deposit and wire transfer scams in IR-2018-253, December 17, 2018.

[23] GAO Report: Tax Fraud and Noncompliance: IRS Could Further Leverage the Return Review Program to Strengthen Tax Enforcement (July 2018) (See https://www.gao.gov/assets/700/693374.pdf).

[24] TIGTA Report: Interim Results of the 2020 Filing Season (April 7, 2020) (See https://www.treasury.gov/tigta/auditreports/2020reports/202045024fr.pdf).

[25] GAO Report: Identity Theft: IRS Needs to Better Assess the Risks of Refund Fraud on Business-Related Returns (January 2020) (See https://www.gao.gov/assets/710/704168.pdf). (GAO Business Fraud Report).

[26] IRS Progress Update, Fiscal Year 2019, p. 23. The high quality of stolen information is a principal reason for a false positive rate of about 65% of the returns identified for further review by IRS IDTTRF fraud filters. See TIGTA Report: The Taxpayer Protection Program Includes Processes and Procedures That Are Generally Effective in Reducing Taxpayer Burden (October 17, 2018).

[27] See GAO Business Fraud Report. "According to IRS data, the average 2018 tax refund for corporations was about $286,200 and about $24,700 for estates and trusts. In contrast, the IRS Data Book, 2018 reports that the average individual tax refund was about $2,900." p. 7.

2015 breach of the Office of Personnel Management (OPM)[28] and 148 million people in the 2017 breach of Equifax.[29] Similarly, Russia has been suspected of disruptive cyberattacks.[30]

In its 9th Annual Cost of Cybercrime Study, Ponemon Institute and Accenture found that cyberattacks are changing in several ways. Targets are evolving, and the impact is moving from the mere theft of data to the destruction or manipulation of data. According to this study, "Attacking data integrity is the next frontier."[31]

The impact of and response to the COVID-19 pandemic should be mined for "lessons learned" and other opportunities

The IRS played a key role in the federal response to COVID-19, including delivering economic impact payments.

The pandemic had a significant impact on "doing business" for the entire tax system – the IRS, states, tax professionals, software and financial services companies, employers and taxpayers. As difficult as it has been, the pandemic creates a firsthand experience to evaluate the resiliency of our tax system and its impact on taxpayers during crisis periods. In that regard, the experience may highlight strengths as well as potential gaps in policies, processes, operations, training, service delivery and many other areas.

ETAAC is unable to conduct an assessment in this area due to the impending statutory deadline for its 2020 Report, but will consider this area for its 2021 Report. Additionally, other stakeholders – including IRSAC – have an opportunity to consider this area, celebrate strengths and identity risks, gaps and opportunities that require attention.

[28] See https://www.nytimes.com/2015/06/05/us/breach-in-a-federal-computer-system-exposes-personnel-data.html.

[29] See https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-four-members-china-s-military.

[30] The so-called NotPetya cyber-attack of June 2017 was distributed through accounting software and allegedly conducted by the Russian military. See https://www.bbc.com/news/technology-40428967 and https://www.zdnet.com/article/russian-military-behind-notpetya-attacks-uk-officially-names-and-shames-kremlin/.

[31] Ninth Annual Cost of Cybercrime Study, p. 6 (March 2019) (See https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf).

ABOUT THE IRS SECURITY SUMMIT

Security Summit: Formation & Structure

The Security Summit was formed in 2015 and includes representatives from the IRS, state tax revenue agencies, tax professional community, tax preparation firms, software developers, financial service companies, and members of the Payroll Community.[32] Additional background information on the Security Summit can be found on irs.gov.[33]

The Security Summit currently has six Work Groups, each of which has a co-lead from each stakeholder group, i.e., the IRS, the states and industry.

The Security Summit initiative also includes a fully operational IDTTRF Information Sharing and Analysis Center (ISAC), which consists of the ISAC Platform (funded by the IRS) and the ISAC Partnership.[34] The ISAC Partnership includes the IRS, state and industry representatives and facilitates collaboration on IDTTRF detection and prevention, and is separately managed through its Senior Executive Board.

The progress of the Security Summit, and the responsibilities, accomplishments and current focus of each Work Group and the ISAC, are further detailed below.

Security Summit: Progress From 2015 - 2019

Five years following the Summit's creation, key indicators on identity theft continue to move in the right direction. Here are key, calendar-year 2019 indicators and how they compare to the 2015 base year:

- The number of taxpayers reporting they were identity theft victims fell 80% based on the number of identity theft affidavits filed.
- The number of confirmed identity theft returns stopped by the IRS declined by 68%.
- The IRS protected a combined $26 billion in fraudulent refunds by stopping confirmed identity theft returns.
- Security Summit financial industry partners recovered an additional $1.7 billion in fraudulent refunds.[35]

Many of the actions taken by the Security Summit partners may be less visible to taxpayers, but are invaluable in the effort to fight IDTTRF. Some of those steps include:

- Improved data analysis. Increased sharing of data points associated with electronic returns that help to identify computer-generated fraudulent returns and

[32] "Payroll Community" refers broadly to employers, software developers, cloud/hosting service providers, payroll service providers, reporting agents and others engaged in payroll and employment tax. "Payroll" is used generically to refer to both the payroll and employment tax areas.

[33] See https://www.irs.gov/newsroom/security-summit.

[34] ETAAC 2018 Annual Report to Congress, p. 2, provides additional background on the ISAC (See https://www.irs.gov/newsroom/electronic-tax-administration-advisory-committee-etaac-annual-reports).

[35] The financial industry have been a key partner in fighting identity theft, helping the IRS and states recover fraudulent refunds that may have been issued. But, as fewer fraudulent tax returns enter the system, fewer fraudulent refunds are being issued.

enable the IRS to stop questionable returns from entering its processing systems.

- More fraud protection. Enhanced IRS identity theft fraud filters, limits on the number of refunds deposited to accounts, and close coordination with financial service providers and debit card companies to identify and return questionable refunds.
- Enhanced Authentication. Stronger measures to authenticate software users, increased collection of information to confirm taxpayer identities, and the creation of multi-factor authentication program to protect IRS online tools.
- Greater outreach and education. Expanded public campaigns to increase awareness of ways to protect against identity theft, including taxpayer and tax professional-focused campaigns such as "Taxes. Security. Together." and "Protect Your Clients; Protect Yourself." Additionally, annual Tax Security Awareness Weeks each December have raised awareness in advance of the tax filing season.
- Expanded information sharing. Created an innovative Identity Theft Tax Refund Information Sharing and Analysis Center (ISAC) that allows the IRS, states and certain trusted tax providers to exchange data about emerging schemes, analyze the data and respond quickly.
- Efforts continue in 2020. Created an online Identity Theft Central online hub[36] that makes it easier for victims to find the information they need.
- Taxpayer-controlled Protections. Expanded the Identity Protections PIN opt-in program to allow taxpayers in 20 states to voluntarily obtain this extra layer of protection.

Work Groups & ISAC: Responsibilities, 2019 Accomplishments And 2020 Focus/Priorities

Communication and Taxpayer Awareness Work Group:

- Responsibilities:
    - Increase awareness among individuals, businesses and tax professionals on the need to protect sensitive tax and financial information.
- 2019 Accomplishments:
    - Developed and continued to conduct an aggressive and multi-faceted social media campaign focused both on taxpayers and the tax professional community highlighting security and protection against identity theft related tax refund fraud and related scams.
        - Instagram: @IRSNews with over 11,000 followers
        - Facebook: published extensively, including IRS Dirty Dozen Tax Scams

[36] See https://www.irs.gov/identity-theft-central.

        - Twitter: @IRSTaxSecurity with over 4,000 followers; hosted dedicated twitter chat #TaxSecurity on December 5, 2019
    - Continued taxpayer focused data protection and security awareness campaign, “Taxes.Security.Together” with emphasis on Cybersecurity to coincide with Nationwide Tax Forums where over 11,000 participants attended six new seminars
        - Cybersecurity for Tax Professionals
        - Tax Security 2.0
        - Identity Theft Victim Assistance; How it Works for You and Your Client
        - Data Compromise Playbook for Tax Practitioners
        - Helping your client steer clear of latest fraud and swindles
        - E-File Identification Number (EFIN) Security Responsibilities
    - Conducted fourth annual Tax Security and Cyber Awareness campaign jointly with industry and state Security Summit partners in collaboration with the tax professional community. Held media and partner events in approximately 30 large and medium-size markets ranging from New York to Los Angeles, San Francisco, Miami, Chicago, Madison, Wisconsin, New Orleans, and Jacksonville, FL.
    - Developed new Partner Toolkit including “do it yourself” new conference script, daily news releases, drop-in articles, social media and more. Designed to allow partners inside and outside the tax community to share information and “message” more widely to their internal members and external audience.

- 2020 Focus/Priorities:
    - Continue to highlight security tips with communications throughout the filing season both in traditional and social media with special emphasis on emerging schemes, rapid response to combat threats and protect data, and what to do when possible data compromise in the tax pro community.

Tax Professional Work Group:

- Responsibilities:
    - Examine how new requirements will affect tax preparers, how the preparer community will be affected by the overall data capture and reporting requirements and how the preparer community can contribute in the prevention of identity theft and IDTTRF.
- 2019 Accomplishments:
    - In collaboration with IRS Return Preparer Office (RPO), delivered basic data security messages directly to PTIN Accounts held by over 700,000 active return preparers.

- Supported RPO communication strategy disseminating availability of continuing education (CE) data protection and security courses via traditional and social media platforms directly to tax professional community.
- With RPO, delivered varied messages to preparer community with different subject lines and at differing times of day and year to determine which messages preparers were more likely to open.
- Worked with Stakeholder Liaison in designing focus group questions for preparers attending 2019 Nationwide Tax Forums.

- 2020 Focus/Priorities:
  - Supporting RPO modification of 2020 Preparer Tax Identification Number (PTIN) registration and renewal application to include language outlining preparer requirements to maintain data and system security standards.
  - Working with RPO in designing an informational handout on security plan basics and available information resources for developing a plan for the 2020 Nationwide Tax Forums.

Strategic Threat Assessment and Response (STAR) Work Group:

- Responsibilities:
  - Identify points of vulnerability (threats/risks) related to the detection and prevention of IDTTRF, develop a strategy to mitigate or prevent these risks and threats, and review best practices and frameworks used in other industries.

- 2019 Accomplishments:
  - Completed Year 3 of a three-year plan implementing the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) for the tax industry.
  - Established a three-year plan to implement the NIST Cybersecurity Framework (CSF) for the Payroll Community sub-group; received four one-year self-assessments from the payroll sub-group.
  - Established a three-year plan to align Trusted Customer requirements with NIST Digital Identity Guidelines.

- 2020 Focus/Priorities:
  - Continue NIST CSF Implementation for Tax Software community and Payroll industry.
  - Conduct a Cybersecurity Tabletop Exercise for the Tax Software community with industry-provided scenarios.
  - Pursue the concept of a unified security approach to provide consistency across the tax ecosystem.

Authentication Work Group:

- Responsibilities:
    - Identify opportunities for strengthening identity assurance and taxpayer authentication practices, including new ways to validate taxpayers and tax return information and new techniques for detecting and preventing IDTTRF.
- 2019 Accomplishments:
    - Analyzed individual return (IMF) authentication data elements stratified across the return population points of origin to further improve selection models and filters and to find correlations between validation of data elements and detection/prevention of identity theft.
    - To enhance customer service in coordination with the tax preparation community, provided industry partners content and actions required by taxpayers for all letters and notices issued by the IRS relating to identity theft.
    - Continued to analyze business tax return data elements and identify next steps to include data element requirements for detection/prevention of identity theft and to further improve selection models and filters.
    - Identified additional data elements related to employment tax returns for inclusion in the business return authentication process.
- 2020 Focus/Priorities:
    - Continue Pilot for Electronic Filing Identification Number (EFIN) Validation Project in preparation for filing season 2020 to provide real time validation and expand the option for validation beyond Security Summit members.
    - Begin development of plan to incorporate NIST and Trusted Customer requirements into business return preparation software.

Financial Services Work Group:

- Responsibilities:
    - Examine and explore additional ways to prevent and deter criminals from accessing tax refunds, tax-related financial products, deposit accounts, and pre-paid debit cards.
- 2019 Accomplishments:
    - Implemented Rejected Direct Deposit Opt-In Program and continued outreach for new member participation in project with dedicated Reject Code (R17) for Automated Clearing House (ACH) refund deposits associated with possible IDT to be frozen to allow for appropriate IDT or Fraud treatment.
- 2020 Focus/Priorities:
    - Update information on National Automated Clearing House Association (NACHA) website and coordination with State Departments of Revenue to

promote participation in R17 Opt-in program both for federal and state tax return refunds.

- Continue evaluating pre-validation and the Treasury Department's Bureau of Fiscal Service pilot efforts to support participation in the external leads program and NACHA reject process.

Information Sharing Work Group:

- Responsibilities:
  - Identify opportunities for sharing information to improve the collective capabilities for detecting and preventing IDTTRF.
- 2019 Accomplishments:
  - Enhanced and automated the Lead submission, analysis, and information sharing process across the industry, state, and federal partnership group and in concert with the IDTTRF Information Sharing and Analysis Center (ISAC).
  - Developed enhanced process and new alert form for the submission of leads and issuance of ISAC Alerts stemming from the Rapid Response Team efforts around suspicious activity requiring immediate action to prevent IDT.
- 2020 Focus/Priorities:
  - Explore opportunities to enhance information and data sharing stemming from passage of the Taxpayer First Act (Section 2003) authorizing expanded authority for the IRS to share federal tax information (FTI) under IRC Section 6103 for the detection and prevention of IDT and tax refund fraud.
  - Collaborate with Authentication Work Group to implement and evaluate data and share information relating to new business return Leads process.

IDTTRF Information Sharing and Analysis Center (ISAC)

- Responsibilities:
  - Centralize, standardize and enhance data compilation and analysis to facilitate sharing actionable data and information.
- 2019 Accomplishments:
  - Created new ISAC enclave to receive, house and share federal tax information with authorized ISAC Partners, which included providing appropriate security protocols tracking data into and out of the enclave, creating specific user accounts to the enclave and providing user guidance on how to use the functionality on the ISAC Portal.
  - At the direction of the IRS, the ISAC created Federal Tax Information (FTI) user accounts for those organizations the IRS has authorized to receive the data.
  - Incorporated data breach information reported to the states or Federation of Tax Administrators on the MOVEiT database on to the ISAC operational

platform (This alignment consolidated information to a single location and allowed for additional analytics).

- Piloted utilizing information from the Secretaries of State to determine linkage with identity theft and test new data sources.
- Integrated the Pre-Validation efforts from the Financial Services Working Group onto the platform. Currently, not all participants exchange data on the platform, efforts continue to migrate others into the platform. The information enables a more holistic view of the patterns/trends associated with this effort.
- Coordinated with the ISAC Analysts Community of Practice to improve the ISAC alerts process to gather more meaningful data to identify threat activity.
- Increased ISAC membership to 72 member organizations including partners and endorsing organizations.

- <u>2020 Focus/Priorities:</u>
  - <u>ISAC Senior Executive Board (SEB):</u>
    - Establish two new key committees:
      - Strategic Planning Committee that will review and revise the ISAC strategic plan.
      - ISAC Analysts Community of Practice Committee – which moved from a steering committee to a full committee due to its highly engaged activities that impact ISAC measurable activities related to identity theft.
    - Continue executing the ISAC's Strategic Goals:
      - *Confidence*: Heighten taxpayers' confidence in the nation's tax systems by knowing that we are all working together to fight identity theft tax refund fraud.
      - *Integrity:* Protect the integrity of the tax ecosystem by preventing and deterring identity theft tax refund fraud.
      - *Collaboration*: Collaborate with partners, endorsers and stakeholders proactively to improve prevention and detection of identity theft tax refund fraud.
      - *Talent Cultivation:* Cultivate a well-equipped, diverse, flexible and engaged cross-functional team throughout the tax ecosystem.
      - *Thought Leadership*: Advance data access, usability and analytics to inform decision making and improve operational outcomes.
      - *Excellence*: Drive increased agility, efficiency, effectiveness and security of the tax ecosystem operations.

- ISAC Operational Platform:
    - Improve User Experience/Utility with appropriate access on a secure platform.
    - Improve training by creating interactive training (teach and do) exercises.
    - Continue efforts to build skills of the community by leveraging the Trusted Third Party, Analyst Community of Practice, endorsing organizations, and membership.
    - Continue efforts to optimize use of the data currently available to the ISAC membership by the creation of new data dashboards.
    - Work with the SEB metrics committee to develop and monitor metrics and measure value added of the ISAC.
    - Continue collaboration with Security Summit Working Groups on opportunities to provide feedback.
    - Continue expansion of the Pre-Validation effort on the ISAC platform and, for those participants not migrating to the platform, identify any barriers.
    - Focus on the implementation of the ISAC-related provisions of the Taxpayer First Act. This includes the development and execution of required MOUs for both industry & MITRE and engagement with the state agency ISAC members for their participation under their existing IRC 6103 authority and agreements with the IRS.
    - Deliver security and safeguard awareness briefings to industry personnel covering their security and safeguard responsibilities and requirements related to their access and use of FTI.

ETAAC Integration With The Security Summit

The Security Summit's efforts were first institutionalized through the auspices of the ETAAC in 2016 when an amendment to ETAAC's charter expanded its scope to include researching, studying and making recommendations regarding the prevention of IDTTRF.

ETAAC's role with respect to the Security Summit was reinforced by Section 2002 of the Taxpayer First Act of 2019 (TFA).[37]

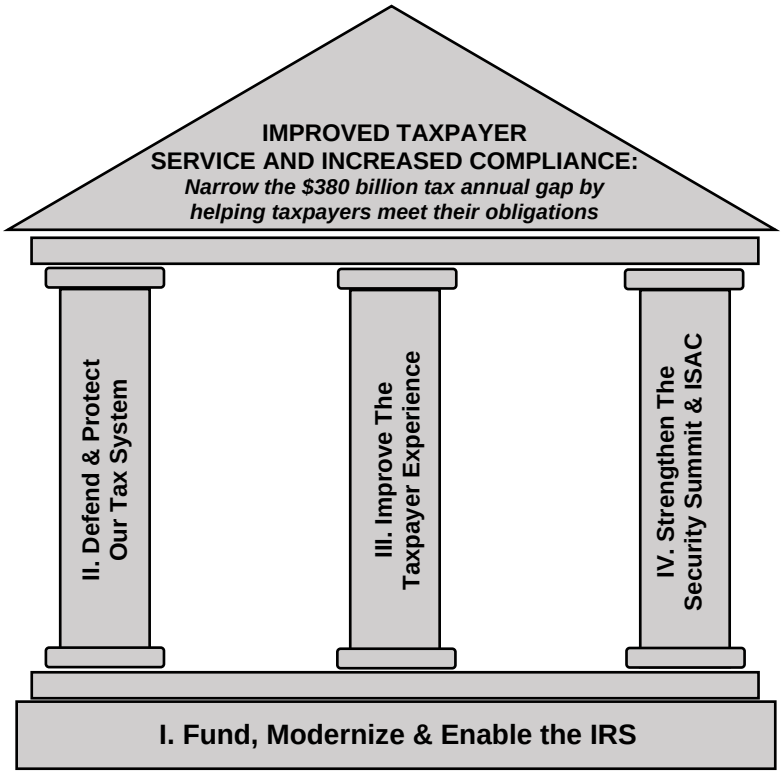
On an ongoing basis, ETAAC members engage with the IRS, as well as with Security Summit membership, by attending and participating in work group activities. Additionally, ETAAC members proactively engage with the Security Summit by consulting with work group co-leads to keep abreast of Security Summit initiatives and IDTTRF developments.

[37] Public Law 116–25 116th Congress (H.R. 3151) signed into law on July 1, 2019.

DETAILED SUPPORT FOR ETAAC 2020 RECOMMENDATIONS

Below are ETAAC's 2020 recommendations and accompanying analysis, which provides important context and elaboration for each recommendation.

As noted above, our recommendations are framed around four themes that build on each other. The first set of recommendations (Part I) focus on building a strong foundation – namely, funding and modernizing the IRS. The remaining three sets of recommendations (Parts II, III and IV) build on that foundation and focus on protecting the tax system, improving the taxpayer experience and fighting IDTTRF by strengthening the Security Summit and ISAC.



I. FUND, MODERNIZE & ENABLE THE IRS

INTRODUCTION

Part I recommends four Congressional actions to enable the IRS to provide high quality taxpayer services, enhance enforcement and build 21st Century capabilities for the IRS.

Recommendations #1 and #2 relate to funding the IRS FY2021 budget request and approving its request for a Program Integrity Cap Adjustment, respectively. **These two recommendations are fundamental to enabling the IRS to narrow the $380 billion annual tax gap and deliver improved taxpayer services. More than ever, our nation needs those uncollected taxes.**

Recommendation #3 relates to Congress monitoring government-wide policies and initiatives intended to enable agencies to implement digital identity solutions, which is critical to all federal agencies especially the IRS.

Recommendation #4 repeats ETAAC's 2019 Recommendation that Congress should provide IRS with the authority and necessary funding to enforce security standards.

……

ISSUES & RECOMMENDATIONS

……

Funding and Modernization

ISSUE: The nation's overwhelming national debt and annual budget deficits require that the IRS narrow the $380 billion annual tax gap – this need has only been amplified by the national response to the COVID-19 pandemic. To accomplish this objective, the IRS requires adequate funding to make it easier for taxpayers to comply, increase its enforcement capabilities, protect the tax system from cybercriminals and other adversaries, and modernize its systems. The IRS is also requesting a $400 million Program Integrity Cap Adjustment for FY2021 to fund additional enforcement capabilities. The IRS estimates a direct return of investment (ROI) on enforcement appropriations of approximately 5:1 and an additional indirect ROI of 11:1 or greater.

RECOMMENDATION #1: ***Fully fund the IRS FY2021 budget request***

Congress should fully fund the IRS's FY2021 budget request to enable the IRS to deliver 21st Century taxpayer experiences, narrow the $380 billion Tax Gap to meet the nation's pressing fiscal needs, protect the tax system and build a modern information system infrastructure. Any appropriations should be allocated across the IRS's four appropriations accounts[38] in a manner to enable the achievement of its stated taxpayer service, enforcement and modernization goals.

RECOMMENDATION #2: ***Consider and approve the IRS's request for an FY2021 Program Integrity Cap Adjustment***

Congress should amend Title 2 U.S. Code § 901 to add the IRS Program Integrity Cap Adjustment to isolate this tax revenue generating opportunity from competing priorities within the Financial Services and General Government appropriations' funding cap. This action will provide a foundational investment for a multi-year effort to restore IRS enforcement levels, increase revenue to the Treasury and strengthen the nation's tax system.

[38] The IRS's four appropriations accounts are: Taxpayer Services, Enforcement, Operations Support and Business Systems Modernization.

Support for Recommendations:

The total federal debt held was already over $21 trillion and projected to grow over $1 trillion annually – before the COVID-19 pandemic expenditures

The federal fiscal situation is unsustainable. The current total federal debt is over $21 trillion.[39] The Congressional Budget Office projects that the federal budget deficit will be over $1 trillion dollars annually between 2021 and 2030, and that public federal debt in 2030 as a percentage of gross domestic product (GDP) will be the highest it has been since the end of World War II.[40]

The cost of responding to the country's needs and risks far exceeds currently available revenues. Domestically, the country expects to incur substantial expenditures to respond to existing healthcare and education needs and to take on new challenges like climate change. Similarly, in foreign affairs, the nation faces new threats from strategic competitors and adversaries, which will impact defense and diplomatic budgets.

The government must generate net revenues beyond just budget cuts and tax increases.

Narrowing the $380 billion Tax Gap is a key strategy to reduce the budget deficit

One clear action to generate more revenue is to narrow the net tax gap, which is estimated to be $380 billion per year.[41] Simply put, the IRS needs to collect more of what is already owed. Importantly, relatively small improvements can deliver big results in terms of federal revenues. For example, a one percent improvement in the voluntary compliance rate, currently estimated at 83.6%,[42] equals about $30 billion a year in federal net revenue.

At the highest level, the IRS needs to do three things: (i) make it easier for taxpayers to comply by providing better taxpayer service and experiences, (ii) collect taxes that are owed but not paid by improving IRS enforcement and collections, and (iii) reduce operating expenses.[43]

Modernization is a key enabler of better service and enforcement and will stabilize rising O&M costs

IRS Integrated Modernization Business Plan

The IRS has a sound approach to modernize. The Modernization Plan will deliver better taxpayer experiences, build a foundation for better revenue collection for the nation's tax system and stabilize growing operations and maintenance (O&M) costs.

---

[39] See https://www.gao.gov/americas_fiscal_future?t=federal_debt.

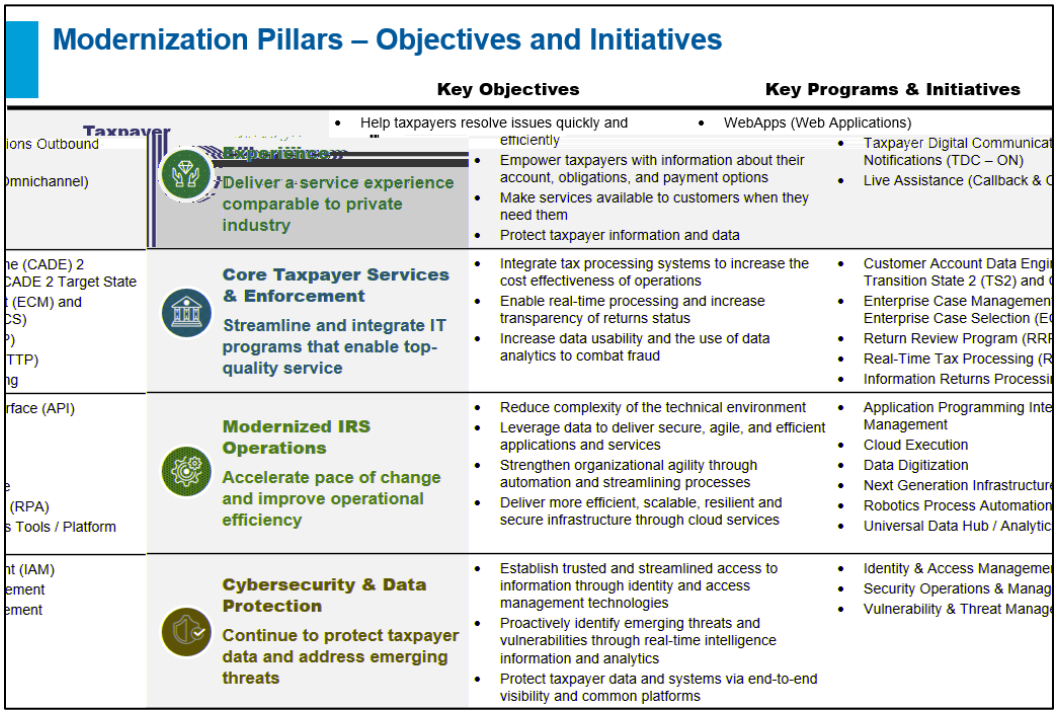
[40] Congressional Budget Office, The Budget and Economic Outlook: 2020 to 2030 (January 2020). (See https://www.cbo.gov/publication/56073).

[41] FY21 IRS Congressional Justification, p. IRS-2.

[42] IRS Progress Update Fiscal Year 2019, p. 19.

[43] To narrow the Tax Gap, former Treasury Secretary Larry Summers recently recommended focusing on three areas: increasing examinations/enforcement, increasing information reporting, and improving information technology and analytics. NBER Working Paper: "Shrinking The Tax Gap: Approaches And Revenue Potential," Summers and Sarin, Nov. 2019 (See https://www.taxnotes.com/special-reports/compliance/shrinking-tax-gap-approaches-and-revenue-potential/2019/11/15/2b47g).

The Modernization Plan includes specific programs and initiatives focused in four key areas: Taxpayer Experience; Core Taxpayer Services & Enforcement; Modernized IRS Operations; and, Cybersecurity & Data Protection.



Modernization Pillars – Objectives and Initiatives

	Key Objectives	Key Programs & Initiatives
Taxpayer Experience: Deliver a service experience comparable to private industry	• Help taxpayers resolve issues quickly and efficiently • Empower taxpayers with information about their account, obligations, and payment options • Make services available to customers when they need them • Protect taxpayer information and data	• WebApps (Web Applications) • Taxpayer Digital Communicat Notifications (TDC – ON) • Live Assistance (Callback & C
Core Taxpayer Services & Enforcement: Streamline and integrate IT programs that enable top-quality service	• Integrate tax processing systems to increase the cost effectiveness of operations • Enable real-time processing and increase transparency of returns status • Increase data usability and the use of data analytics to combat fraud	• Customer Account Data Engi Transition State 2 (TS2) and • Enterprise Case Managemen Enterprise Case Selection (E • Return Review Program (RR • Real-Time Tax Processing (R • Information Returns Processi
Modernized IRS Operations: Accelerate pace of change and improve operational efficiency	• Reduce complexity of the technical environment • Leverage data to deliver secure, agile, and efficient applications and services • Strengthen organizational agility through automation and streamlining processes • Deliver more efficient, scalable, resilient and secure infrastructure through cloud services	• Application Programming Inte Management • Cloud Execution • Data Digitization • Next Generation Infrastructur • Robotics Process Automation • Universal Data Hub / Analytic
Cybersecurity & Data Protection: Continue to protect taxpayer data and address emerging threats	• Establish trusted and streamlined access to information through identity and access management technologies • Proactively identify emerging threats and vulnerabilities through real-time intelligence information and analytics • Protect taxpayer data and systems via end-to-end visibility and common platforms	• Identity & Access Manageme • Security Operations & Manag • Vulnerability & Threat Manag

The taxpayer experience is at the core of the Modernization Plan. Although the plan will take several years to fully implement, the IRS is making strong progress in delivering services such as customer callback, webchat, secure messaging and others that will improve the taxpayer experience. The plan will also enable IRS employees and tax practitioners to provide efficient, high quality service. These capabilities and others will remain priorities in the IRS's customer service strategy and information technology strategic plan that are under development pursuant to the Taxpayer First Act.[44]

The Modernization Plan will deliver other key benefits as well, including: expanding taxpayer access to information, reducing call wait and case resolution times, expediting return and refund processing with real-time return processing and taxpayer error correction, simplifying identity verification to expand access to online services while protecting data, increasing systems availability for taxpayers and practitioners, and facilitating the implementation of new tax provisions by eliminating millions of lines of legacy code. The plan will also improve the foundational technology used by IRS employees to interact with taxpayers, retire legacy systems and automate more manual and paper-based processes.

IRS is pursuing modernization in an open, transparent and collaborative way

One of the IRS's key insights from its first year of plan execution was the value of a strong partnership and frequent communications with oversight groups and key stakeholders, including the GAO and Congressional staff.

[44] See TFA Sections 1101 and 2101.

The IRS's modernization efforts will be further enhanced with the development of its information technology strategic plan, periodic updates and independent verification pursuant to the Taxpayer First Act.

The Modernization Plan is already delivering an impact – FY2019 and FY2020 benefits

In the first year of the Modernization Plan (FY2019), the IRS used Congressional funding to deliver dozens of new technology and cybersecurity capabilities that directly benefit taxpayers and practitioners, including: Customer Callback on certain IRS phone lines, which improved the customer experience by reducing caller wait times[45]; an ID Verify Tool that enables legitimate taxpayers to clear their return remotely without having to call or visit an IRS office; improved Return Review Program models and filters based on new schemes to prevent IDTTRF, which protected more than $2 billion in revenue between January and September 2019; and, a redesigned Tax Withholding Estimator that provides taxpayers with a mobile-friendly online tool to estimate their tax liability and fine-tune their federal withholding.[46]

For FY2020, the IRS received about half of its request for Business Systems Modernization. However, using carryover funds and user fees to help close the funding gap, the IRS expects to deliver several additional benefits including: adding customer callback to more IRS phone lines and applications for an average 11.3 million calls/year; introducing robotics to automate more manual processes[47]**;** and, continued cybersecurity enhancements. (See Appendix C)

IRS FY2021 budget reflects commitment to service, enforcement & modernization

FY2021 base budget request

The IRS's FY2021 base budget request is $12 billion to administer the nation's tax system and collect more than $3.6 trillion in gross taxes to fund the government and strengthen tax compliance. The IRS's request is broken into four appropriations accounts: Taxpayer Services, Enforcement, Operations Support and Business Systems Modernization.

Appropriation Account ($ in Millions – some rounding)	**FY20 (Enacted)**	**FY21 (Requested)**	**YOY Change**
Taxpayer Services	$2,536	$2,562	$26
Enforcement	$4,909	$5,071	$162
Operations Support	$3,885	$4,105	$220
Business Systems Modernization	$180	$300	$120
Total Appropriated Resources	**$11,510**	**$12,038**	

[45] When offered the option, 77% of customers chose a callback vs. 55% industry standard.

[46] The IRS was very successful in taking a collaborative approach to the design of this tool by holding numerous discussions with outside stakeholders to gain their input.

[47] For example, using robotics, IRS procurement can now complete certain compliance checks in as few as five minutes, which results in an aggregate time savings of up to 17,625 hours per year. Another illustration is the automation of monitoring compliance of Offers in Compromise to track taxpayer filing and payment compliance during the five years after an offer has been accepted.

The FY2021 budget request includes $300 million for critical modernization projects, which are funded in programs and projects in both the Business Systems Modernization and the Operations Support appropriations accounts. Two of the most critical projects funded in the Business Systems Modernization Account are Customer Account Data Engine 2 ($100 million) and Enterprise Case Management ($64 million), which will enable better taxpayer services, enforcement and collections.

Full funding of the Business Systems Modernization and the Operations Support accounts is critical for the IRS's fight against IDTTRF. These appropriations accounts fund key technologies and systems that enable the IRS to detect potential IDTTRF returns and for legitimate taxpayers to verify their returns so their refunds can be released.[48] Additionally, they fund another key underlying technology – the IRS Secure Access Digital Identity platform, which is essential to enable taxpayers to use IRS online and mobile solutions safely and securely.

In some respects, Congress and the IRS are in a "you can pay me now, or you can pay me later situation." The cost of maintaining the IRS's current legacy systems is on an unsustainable trajectory. Basic operations and maintenance costs exceed $2.2 billion a year and, with no action, are projected to top $3 billion in FY2027, which will divert resources from needed taxpayer services and enforcement efforts. All of these O&M expenses are in the Operations Support account, and the situation reinforces the urgency of the IRS's request for $300 million for modernization.

FY2021 Program Integrity Cap Adjustment

The Program Integrity Cap (PIC) Adjustment is a revenue generating investment – the government spends some money to save or generate even more money.

In addition to its FY2021 base appropriations, the IRS has proposed a $400 million PIC Adjustment to fund investments to expand and improve the IRS's overall tax enforcement program.[49]

These investments are designed to narrow the $380 billion tax gap. If approved, the PIC Adjustment would fund 19,300 additional staff over a five year period and restore IRS enforcement capabilities (which are quantifiable by several performance measures) to historical levels. The IRS estimates that these incremental investments would generate $79 billion in new revenue over 10 years at a cost of $15 billion resulting in net revenue of $64 billion over 10 years. This return on investment (ROI) is likely understated because it does not reflect the effect that enhanced enforcement has on deterring non-compliance. IRS Research has estimated that the indirect impact on collections is on the order of 11+ times the direct revenue collections.[50]

---

[48] Some of the key IDTTRF-related systems support the Return Review Program (RRP), the Taxpayer Protection Program (TPP) and the Security Summit. Related technologies include the Discoverer Replacement/Palantir Solution (used by IDTTRF analysts to make selections to TPP that may not be identified by RRP during the filtering process), IDVerify, and the EFIN validation API. Full funding would enable the IRS to consider additional initiatives such as Taxpayer Account Lock/Unlock and the replacement of EFDS Legacy Components.

[49] The IRS PIC proposes $280 million for the Enforcement account and an associated $120 million for the Operations Support account. Additional adjustments are provided in future years to fund new initiatives and inflation.

[50] Generally, IRS "investment ROIs" are based on IRS total enforcement revenue collected divided by IRS total appropriations and on additional IRS studies.

A PIC Adjustment is typically considered by the Budget Committees which, if approved, would specifically provide for that amount in the appropriations caps set in their budget resolutions or any enacted budget agreement. This procedural step enables the Financial Services and General Government (FSGG) appropriations subcommittees to increase their 302(b) cap by the specified amount.[51]

However, the IRS's FY2021 PIC Adjustment cannot and will not be considered unless Congress takes some actions outside of the normal process.

Specifically, the FSGG appropriations subcommittees have no clear path to appropriate the additional dollars for the IRS's PIC Adjustment because the Bipartisan Budget Act of 2019 enacted in August 2019 prospectively specified caps for not just for FY2020, but also for FY2021 without anticipating the potential of an IRS PIC Adjustment. In effect, the Bipartisan Budget Act of 2019 obviated the need for the Budget Committee to convene to decide FY2021 caps and exceptions.

Under the circumstances, some type of separate legislative action is required to allow the appropriations committees to enact a bill to include the IRS's PIC Adjustment.

Congress should be aware of several key factors as it considers the IRS's FY2021 budget request

The need for consistent appropriations

The single most important factor affecting the IRS's ability to stay on track with modernization is the certainty and timing of full-year funding. The IRS did not receive full funding for modernization in FY2020. As a result, at the beginning of FY2020, the IRS was held to prior year spending levels under a continuing resolution, which assumed a lower full-year funding level. The IRS was compelled to intentionally pause or adjust work to avoid spending funds it might not have received, which delayed the modernization effort and required the IRS to play catch up.

The need for balanced appropriations

ETAAC asks that Congress be mindful of three key considerations in allocating appropriations across the IRS's four appropriations accounts. If appropriations between the accounts are not adequately balanced, the IRS is required to request inter-appropriations transfers which slow its progress and increase execution costs.[52]

First, please don't think of the Operations Support account as an "overhead" account. It actually plays a key role in enabling taxpayer services and enforcement activities by funding critical information systems and telecommunications support development, security and maintenance. This account also funds necessary shared services (such as facilities services, rent, printing, postage, and security) and other policy and management activities.

---

[51] The Congressional Budget and Impoundment Control Act of 1974 established the current budgeting system. Sections 302(a) and 302(b) of that law describe budgetary caps, which are referenced by the budget community as short-hand for the allocations/caps. See also http://www.crfb.org/papers/appropriations-101.

[52] It may be appropriate for Congress to consider adjusting the thresholds that require Congressional approval to transfer or reprogram funds to increase IRS efficiency.

Second, the IRS cannot just "hire" its way into increasing audit coverage and improving customer service. Technology investments are inextricably tied to taxpayer service and enforcement initiatives. For example, revenue agents need a computer and software to conduct research and audits, network and telecom support to interact with taxpayers by phone, mobile devices to stay connected while in the field, office space to work and travel funds. All of these expenses are covered by appropriations to the Operations Support account. So, an imbalance is created when the IRS receives increased enforcement funding to hire more revenue agents and officers but reduced funding in Operations Support. It is analogous to purchasing a new car but having no money left for fuel or maintenance.[53]

Finally, IRS information technology is funded by both the Business Systems Modernization (BSM) and Operations Support accounts. It takes more than just BSM funding for the IRS to fully modernize. The IRS relies on the Operations Support account to implement technology changes to support the Taxpayer First Act and fund other critical services and initiatives. For example, the Operations Support account funds the Return Review Program, which is the agency's primary fraud detection system. It also funds efforts to update existing services like the Tax Withholding Estimator, improve Secure Access identity verification capabilities and expand the IP PIN program nationwide.

Building IRS enforcement capabilities will take time, so policymakers should act now

To narrow the tax gap, the IRS must improve its enforcement capabilities, which requires an investment in both people and technology. Regarding people, staff needs to be hired, on-boarded and trained and, then, continuously developed over time. This effort does not happen overnight – the IRS must start hiring and training now if policymakers want the IRS to hit on all cylinders in 3-5 years.[54]

Other circumstances can dilute taxpayer service and enforcement appropriations

The impact of increased appropriations on taxpayer service and enforcement can be diluted or crowded out by several factors, including:

- Inflation and labor cost increases. The IRS's FY2021 budget request includes $452 million for the IRS to "self-fund" inflation and significant labor (wages, pension contributions, etc.) costs relating to current activities and the annualization of the 3.1 percent pay raise from Congress.
- IDTTRF and Cybersecurity higher share of budget. Increasingly sophisticated fraud schemes and cybercriminals threaten IRS systems and require the IRS to increase IT security efforts. Currently, the IRS spends around $330 million on cybersecurity and $450 million on identity theft.

[53] Similarly, customer service representatives funded in the Taxpayer Services account use telephone lines and computer systems and work in facilities funded through the Operations Support account.

[54] The IRS's staffing challenges are exacerbated by its aging workforce and the high percentage of its employees reaching retirement age. See https://federalnewsnetwork.com/workforce/2019/04/irs-commissioner-aging-workforce-lost-an-entire-generation-to-hiring-freeze/.

- Unfunded and under-funded legislative mandates consume existing resources. The implementation of key legislation, especially when not accompanied by funding, requires the IRS to reallocate funds from other planned activities. For example, the IRS's FY2021 request includes $106 million to implement the Taxpayer First Act which will revamp customer service, introduce new taxpayer protections, and deliver new online service platforms to facilitate filing and payment for individuals and businesses.

ETAAC supports full funding of IRS's FY2021 request and PIC Adjustment

ETAAC recommends that Congress fully fund the IRS's FY2021 budget request with consistent, balanced, multi-year appropriations to support the IRS's taxpayer service, enforcement and modernization efforts. Additionally, ETAAC recommends that Congress take legislative action to approve the IRS's FY2021 PIC Adjustment.

……

Digital Identity Implementation Across Federal Agencies

ISSUE: Digital identity is the ability to remotely identity proof and authenticate persons. This capability is a critical dependency for any federal agency, including the IRS, to provide modern electronic services. It is the front door to any personalized online and mobile services. The capability must be both secure and accessible, which is difficult to achieve in these times. Making progress in this area presents government-wide challenges that warrant Congressional attention and support.

RECOMMENDATION #3: ***Monitor and enable government-wide digital identity policies and initiatives***

Congress should monitor the direction and progress of government-wide digital identity policies and initiatives, and provide legislative and funding support as necessary.

Support for Recommendations:

IRS electronic services require secure, accessible and compliant identity solutions

Recent ETAAC Reports have discussed the IRS's need to provide digital and mobile services to meet taxpayer and other stakeholder needs and expectations. Because many of these services cannot be provided without effective digital identity solutions,[55] the IRS has prioritized digital identity initiatives as an element of its Strategic Plan FY2018 – FY2022 (IRS Strategic Plan).[56] Additionally, the digital identity area is evolving rapidly, which will require ongoing IRS collaboration in this area.[57]

[55] Digital identity, and its subcomponents, are referred to in several ways including e-authentication, identity verification, identity assurance and identity proofing. See NIST SP 800-63 *Digital Identity Guidelines* (https://pages.nist.gov/800-63-3/).

[56] See https://www.irs.gov/pub/irs-pdf/p3744.pdf.

[57] See ETAAC's 2020 Recommendation #8.

OMB Memorandum M-19-17 establishes federal policy in identity management

In 2017, NIST set the technical requirements for digital identity in NIST SP 800-63-3, and the IRS has taken a systematic and comprehensive approach to implement these requirements.

In 2019, the Office of Management and Budget (OMB) issued Memorandum 19-17, which consolidates Federal Identity Credential and Access Management (ICAM) policy into a single source of direction and guidance for federal agencies including government-to-government federation and public facing identity solutions.[58]

Most relevant to the IRS's initiatives are specific mandates on public facing identities that direct agencies:

- To comply with NIST SP 800-63 and implement risk management processes for determining its assurance levels;
- To use federal and commercial shared services for public facing identity solutions;
- To use federated identity solutions to support the use of credentials across government agencies and properties;
- To enable citizens to use commercially available authentication options; and,
- To create application programming interfaces (APIs)[59] to allow – where permissible by law - other agencies and commercial entities to make use of data for identity proofing purposes

Delays and potential gaps in OMB M-19-17 implementation are slowing agencies

OMB M-19-17 has assigned key responsibilities to designated government entities, including mandates for the (i) Department of Commerce to establish, develop, and maintain resources for federation protocols, identity proofing, and authentication in alignment with NIST SP 800-63, and (ii) the General Services Administration (GSA) to develop accreditation criteria for products and services that meet NIST 800-63 assurance levels.

These designations, although necessary, create new dependencies for agencies working to implement digital identity solutions. Any delays in execution by those designated agencies can slow down the execution of others. For example, the IRS cannot implement external commercial Credential Service Providers that are not properly certified by a government agency in accordance with OMB M-19-17. OMB M-19-17 splits responsibility for the certification process between NIST and GSA, but no deadline has been set for an operational program/process. As a result, the transition by

[58] See https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf. OMB M-19-17 formalizes concepts covered in previous informal directives (e.g., Federal CIO memos, Executive Orders) and updates those described in previous OMB Memo 04-04. It rescinds and supersedes many of these prior initiatives.

[59] Generally, an API is a set of definitions and protocols for building and integrating application software that enable different applications and systems to work together more seamlessly, e.g., transfer data.

the IRS to its new digital identity platform[60] is delayed until Credential Service Provider certifications are approved.

OMB M-19-17 also directs federal agencies to use shared services, to the extent available, to deliver identity assurance and authentication services to the public. Although the memo states that agencies should "share proofing confirmations across agencies to reduce public burden" with "appropriate consent and privacy protections," OMB M-19-17 does not provide a clear structure for how to share those confirmations. For example:

- No Federal Trust Framework Across Agencies. To enable the adoption of shared services, a common set of requirements is needed to establish a minimum level of trust and common expectations across agencies. The IRS is in the process of establishing an External Identity Federation Trust Framework that outlines guidelines and requirements for how the IRS will federate and accept authentication assertions from external (i.e., non-IRS) CSPs. This document will delineate the relationship between CSPs and the IRS whenever the IRS receives credentialing services from an external entity, including other government agencies. However, without an overall shared trust framework, agencies may establish separate frameworks with varying guidelines and requirements, which could make it difficult to share proofing confirmations across federal agencies. Alternatively, a shared Federal Trust Framework created through engagement among agencies could provide high level guidance that each agency could use as a starting point for its own trust frameworks based on individual risk thresholds. This shared starting point would allow agencies to consume services and proofing confirmation without unnecessary cost and customization while ensuring compliance with one another.
- No Shared Services Roadmap. While GSA provides an identity playbook on Login.gov that outlines principles for identity management systems and information about how to partner with Login.gov for CSP services, there is no document that outlines a high-level roadmap for sharing services across agencies. Such a document should address key items such as robust fraud monitoring, incident management, budget coordination, and privacy principles relevant to shared proofing confirmation.

While the IRS is exploring and testing solutions, agency collaboration is needed as each explores potential CSP needs to increase the likelihood of successfully sharing proofing confirmation across agencies. This would reduce the burden for individuals logging in for services across the federal government. Given that, there may be an opportunity to design a steering group or other mechanism to help identify gaps and potential solutions across agencies. The IRS has scheduled a meeting with other federal agencies, including General Services Administration (GSA), Veterans Affairs (VA), Health & Human Services (HHS), Treasury, and Social Security Administration (SSA) to discuss this topic. However, it seems that execution in this area could be enhanced by a high-

[60] IRS is transitioning from a non-compliant platform (Secure Access) to a platform that will meet the NIST 800-63-3 requirements (Secure Access Digital Identity or "SADI").

level implementation strategy with goals, fraud monitoring principles, and a timetable accompanied by more transparent progress reporting.

Congressional attention to the progress of digital identity strategy & initiatives is warranted

Congress has recognized that digital identity is a government-wide challenge.

It recently asked GAO to review federal agencies' remote identity proofing practices in light of the then recent Equifax breach and the potential for fraud.[61] GAO's objectives included understanding and assessing the risks and effectiveness of federal practices for remote identity proofing, as well as the sufficiency of federal identity proofing guidance. After conducting its review, GAO made recommendations to strengthen online identity verification processes in a variety of areas including the reporting of progress in adopting secure identity proofing practices.

ETAAC believes continued Congressional attention is warranted in this area. There are opportunities to gain insights concerning the development and implementation of digital identity shared services and to monitor the progress of agencies responsible for enabling the requirements of OMB M-19-17. For example, to enable more regular evaluation of this area, GAO might consider adding digital identity to its list of "critical actions needed" pursuant to its High Risk Series topic of "Ensuring the Cybersecurity of the Nation."

Finally, increased, dedicated funding for government-wide digital identity shared services and shared service programs would enable the government to develop leading edge services to advance the OMB mandates and improve the security and user experience of digital identity services.

……

IRS Authority Regarding Security Standards

ISSUE: Our federal tax system is under cyber-attack every day. The end-to-end public and private tax system must be secure. To achieve that objective, the IRS must lead a coordinated effort to understand the risks to the tax system, and develop and execute an effective cybersecurity strategy. The IRS's success in this area requires it to have clear authority and adequate funding.

RECOMMENDATION #4: *Provide IRS with the authority and necessary funding to enforce security standards*

Congress should grant the IRS the clear legal authority and provide the associated funding to issue and enforce appropriate information security standards and guidance in the area of tax administration, which could include adopting existing or establishing new administrative, technical and physical safeguards, implementing required education and training, and providing ongoing guidance.

[61] GAO Report "Data Protection: Federal Agencies Need to Strengthen Online Identity Verification Processes" (May 2019) (See https://www.gao.gov/assets/700/699195.pdf).

Support for Recommendation:

ETAAC and GAO have recommended that the IRS take action regarding third-party cybersecurity – but IRS has raised barriers to action

ETAAC has recommended that the IRS take action to improve the security in the tax system as long ago as 2011.[62] More recently, it has made several security-related recommendations in its last three Reports,[63] as well as this year (See Recommendations #6 and #7 below).

Similarly, last year, GAO completed a study of the IRS's oversight of third-party security, and offered several recommendations for IRS action.[64]

In its initial response to GAO, the IRS disagreed with five of GAO's eight recommendations. Overall, the IRS stated that it does "not have the statutory authority to establish data security requirements and enforce compliance with those requirements on third-party transactions or relationships." Further, for this and other reasons,[65] the IRS declined to act in several areas including: developing a governance structure to coordinate the IRS's efforts to protect taxpayer information while at third-party providers[66]; updating the IRS's monitoring programs for electronic return originators; and, conducting a risk assessment to determine whether different monitoring approaches were appropriate for all of the provider types in the IRS's Authorized e-file Provider program.[67]

It does appear that no single provision of the Internal Revenue Code provides the IRS with explicit authority to regulate the standards for e-file providers, although the IRS may have the implicit authority to protect the integrity of the e-file system by regulating e-file providers insofar as their activities relate to electronically filing returns.[68] For example, the IRS has exercised this authority by supplementing the FTC Safeguards Rule with six security-related standards for online providers under the IRS Authorized e-file Provider Program.[69]

---

[62] 2011 ETAAC Report to Congress, Recommendation #1.

[63] 2017 ETAAC Report to Congress, Recommendations #17-21; 2018 ETAAC Report to Congress, Recommendations #5-10; and, 2019 ETAAC Report to Congress, Recommendations #6-7.

[64] GAO Report: Taxpayer Information: IRS Needs to Improve Oversight of Third Party Cybersecurity Practices (May 2019) (See https://www.gao.gov/assets/700/699000.pdf) (GAO Third Party Cybersecurity Report).

[65] IRS's principal view was that it lacked explicit statutory authority and funding, or that the requested action in the absence of such authority would be inefficient, ineffective and a costly use of limited resources.

[66] ETAAC has previously referenced the lack of centralized ownership or coordination as an issue in this area because ETAAC believes it adversely impacts Security Summit initiatives. See 2018 ETAAC Report to Congress, Recommendation #10, and related observations in 2019 ETAAC Report to Congress, p. 40.

[67] In contrast, in an unrelated audit, the IRS agreed with several TIGTA security-related recommendations relating to IRS VITA programs, e.g., develop information security plans, issue security plan templates and conduct knowledge checks. TIGTA Report, Actions Are Needed to Improve the Safeguarding of Taxpayer Information at Volunteer Program Sites, pps. 23 – 29 (November 13, 2019). It is unclear to ETAAC why IRS could take many of the comparable actions in the TIGTA situation, but not in the situation described in the GAO Report.

[68] See GAO Third Party Cybersecurity Report, p. 18.

[69] See IRS Pub. 1345, p. 6.

Congress should provide IRS clear authority to set security standards with adequate funding

Provide clear authority

The nation's ability to protect its public/private tax system from disruption and cyberthreats[70] is directly and adversely affected by the absence of clear IRS authority and funding, which restricts its attention to this vital area.

ETAAC agrees that the IRS having explicit authority to establish security standards for tax preparers would enhance its ability to protect taxpayer information and mitigate the risk of legal challenges. For that reason, ETAAC believes that Congress should make explicit the IRS's statutory authority to set and enforce security standards in the area of tax administration.[71]

The IRS's FY2021 Congressional Justification includes a legislative proposal to provide the Treasury Department (IRS) with the explicit authority to regulate all paid tax return preparers.[72]

ETAAC agrees with this proposal with three clarifications. First, the IRS's legislative proposal focuses on the promotion of "high quality services from paid tax return preparers," which presumably would have the IRS assessing the service level and quality of preparers. ETAAC understands this proposal may raise criticisms of government overreach or other policy positions that reduce the likelihood of its eventual enactment. ETAAC strongly believes the IRS's authority should, at a minimum, include the ability to set and enforce security standards for taxpayer data[73] even if any eventual authority granted to the IRS does not extend to the unlimited regulation of all paid preparers. Second, any information security oversight authority granted to the IRS should extend to voluntary tax preparers providing services under IRS programs, such as VITA and TCE, not just to paid preparers. Third, any authority to oversee information security should extend to business returns, not just individual returns.

Provide adequate funding

The regulation of third-party cybersecurity in the tax system would be an entirely new responsibility for the IRS. Therefore, in connection with any grant of authority, Congress must also provide corresponding funding to the IRS appropriate to the task. The IRS would be in a better position to scope the resources required to execute an appropriate third-party cybersecurity program if it completed the study that ETAAC has called for in Recommendation #7 of this Report.[74]

---

[70] See 2020 ETAAC Recommendations #5, 6 and 7 in this Report.

[71] ETAAC made a similar recommendation in its 2019 Report to Congress (See Recommendation #7 asking Congress to grant to IRS the clear authority to develop, implement and enforce appropriate information security standards and practices in the area of tax administration.)

[72] See FY21 IRS Congressional Justification, p. IRS-35.

[73] Many recent Congressional bills concerning preparer regulation have not extended to developing and enforcing security standards, , e.g., Section 2 "Regulation of Tax Return Preparers," Senate Bill S. 1192 – Taxpayer Protection and Preparer Proficiency Act of 2019 introduced into the 116th Congress (2019-2020). (See https://www.congress.gov/bill/116th-congress/senate-bill/1192/text).

[74] ETAAC made a comparable recommendation in its 2019 ETAAC Report to Congress, Recommendation #6.

II. DEFEND & PROTECT OUR TAX SYSTEM

INTRODUCTION

The recommendations in Part II focus on ensuring the uninterrupted, secure operation of our nation's system tightly integrated electronic tax administration system, which is reliant on both government and private sector actors.

Recommendation #5 relates to identifying and mitigating disruption threats to the end-to-end tax system, which appears to present a planning gap. Recommendation #6 encourages the IRS to promptly engage with the FTC and tax community to assess the impact and implementation of the FTC's proposed changes to Safeguards Rule, which a significant majority of the tax preparer community do not understand and are not equipped to comply. Finally, Recommendation #7 recognizes the gap in the IRS's understanding of the security risks and vulnerabilities in the tax preparer community, and repeats ETAAC's 2019 recommendation for a study in this area.

……

ISSUES & RECOMMENDATIONS

……

Protecting the Tax System and Its Supply Chain

ISSUE: Every year, the federal tax system generates about $3.5 trillion dollars in collections that fund about 95% of government operations and deliver approximately $350 billion in tax refunds. That system is under attack every day. Although current attackers seem to be focused on monetary gain, **future attacks could shift to disrupting government operations and the economy**. The IRS needs to consider overseeing a kind of tax system-wide business continuity plan.

RECOMMENDATION #5: ***Collaborate on the identification and mitigation of disruption threats to our tax system***

The IRS should work with the Security Summit to evaluate and develop responses to potential attacks by adversaries intended to disrupt our tax system and, thereby, interrupt the flow of government revenues and tax refunds.

Support for Recommendation:

The tax system is critical to the U.S. government, economy and taxpayers

The nation relies on a highly integrated end-to-end public/private electronic tax system built on systems created and operated by federal and state governments as well as the private sector. Generally, tax returns are created by taxpayers enabled by the private sector, and transmitted to the IRS and state revenue agencies. Only a relative handful of individual tax returns are manually prepared and mailed by taxpayers using IRS forms and publications, a pen and calculator.

At the macroeconomic level, the tax system has a huge impact on the government and economy. During the 2019 filing season, the IRS collected over $3.6 trillion in gross taxes, processed about 255 million federal tax returns and forms, and issued over $300 billion in income tax refunds to about 110 million individuals and families. The IRS generated 95 percent of the funding that supports the federal government's operations.

At the individual consumer level, the average refund per household was about $2,800 -- 90 percent of which were issued within 21 days of filing. Any disruption in refund issuance puts pressure on those Americans already struggling to pay relatively small, unexpected expenses such as a car repair or broken refrigerator, because of the lack of savings or access to affordable credit.[75]

Cybercriminals remain a key threat to the economy and tax system

Cybercrime continues to increase. Between 2014-2018, the FBI's Internet Crime Complaint Center (IC3) received a total of 1,509,679 complaints accounting for an estimated $7.45 Billion in losses. IC3's most recent data reflected a 16% increase in complaints and a 90% increase in associated losses.

Identity Theft Tax Refund Fraud (IDDTRF) has been the principal manifestation of cybercrime in the tax system. Fortunately, the efforts of the IRS, states and private sector through the IRS Security Summit have significantly reduced IDTTRF in the individual tax system. Not surprisingly, cybercriminals continue to look for other financial opportunities in the tax area. As a result, the IRS is seeing increases in IDTTRF-related activities in the areas of business tax schemes and the theft of sensitive personal and tax return information from tax preparers, businesses, human resources departments and others.

Adversaries focused on disrupting the tax system could pose an even greater threat

Cybercriminals are only one element of the threat. There have also been allegations of nation state involvement in cyberattacks.

As noted above, China and Russia have been suspected or accused of past cyberattacks. Then, just a few months ago, the State Department issued a press statement accusing Russia of conducting cyberattacks to disrupt government and private web sites and broadcast stations in the country of Georgia.[76]

In its 9th Annual Cost of Cybercrime Study, Ponemon Institute and Accenture found that cyberattacks are changing in several ways including (italics added):

- Evolving targets: Information theft is the most expensive and fastest rising consequence of cybercrime—but *data is not the only target. Core systems, such as industrial control systems, are being hacked in a powerful move to disrupt and destroy.*

[75] See https://www.federalreserve.gov/publications/2019-economic-well-being-of-us-households-in-2018-dealing-with-unexpected-expenses.htm.

[76] See https://www.state.gov/the-united-states-condemns-russian-cyber-attack-against-the-country-of-georgia/.

- Evolving impact: While data remains a target, theft is not always the outcome. *A new wave of cyberattacks sees data no longer simply being copied but being destroyed — or changed — which breeds distrust. Attacking data integrity is the next frontier.*

Typically, discussions about attacks on core or critical infrastructure focus on electrical grids, telecommunications networks and the banking system.

The tax system should be part of that discussion given the potential adverse impact of its disruption on our government's fiscal operations, economy and taxpayers.

IRS should extend its evaluations of overall tax system risks to include disruption threats

As it should, IRS is currently focused on protecting taxpayer information in its systems and, in varying degrees, improving the cybersecurity of the tax industry. However, the threat to the tax system goes beyond protecting information in the possession of IRS or even in the tax industry.

ETAAC believes that the IRS needs to expand its view of the tax system, and consider what actions need to be taken (government and private sector) to be prepared to protect our tax system from disruption attacks and to recover from them. The IRS needs a thoughtful, comprehensive approach to developing a sort of business continuity plan (BCP) for our tax system. As it defines "preparedness" for its internal BCP efforts, the IRS should consider the range of deliberate, critical tasks, and activities necessary to build, sustain, and improve the tax system's operational capability to prevent, protect against, respond to, and recover from domestic incidents.[77]

To that end, the IRS should work with the tax system's stakeholder communities to evaluate comprehensively how adversaries could disrupt the tax system in terms of revenue collection, tax submission and processing, and refund disbursement. Necessarily, this type of evaluation must also consider third-party risks or dependencies of the overall tax system. The effort should encourage out-of-the-box creativity such as that associated with purple team exercises, rather than using more controlled approaches such as scripted interviews or table top exercises.[78] Any review needs to look beyond individual systems and consider how these systems work together dynamically.

……

FTC Safeguards Rule

ISSUE: The FTC Safeguards Rule mandates security requirements for tax preparers including consumer tax software and tax preparers serving consumers (paid commercial and unpaid volunteers). The Rule is enforced by the Federal Trade Commission (FTC) and currently provides relatively high level requirements. As cybersecurity threat has increased, the FTC has reconsidered the adequacy of the existing Rule and issued a

[77] Internal Revenue Manual (IRM) Section 10.6.1 Overview of Continuity Planning (See https://www.irs.gov/irm/part10/irm_10-006-001).

[78] For more on "purple teaming" (vs. red and blue teaming), see https://danielmiessler.com/study/red-blue-purple-teams/ and https://www.fireeye.com/services/purple-team-assessment.html.

proposed rule that would substantially increase its requirements. The impact of these changes on the tax preparation industry is unknown.

RECOMMENDATION #6: *Engage with the FTC to assess impact and implementation of proposed changes to FTC Safeguards Rule*

The IRS should work with the FTC and tax preparation community (including VITA/TCE) to understand the substance and impact of the FTC's proposed amendments to the FTC Safeguards Rule, and implement a plan to educate and enable the tax preparation community to comply with any new security requirements without the significant and unnecessary disruption of this community's ability to serve taxpayers.

Support for Recommendation:

The FTC Safeguards Rule is the primary security regulation for tax preparers

Consumers rely on a highly integrated electronic income tax preparation community to meet their individual income tax filing obligations. Of the approximately 150 million individual returns filed every year, about 90 million are prepared by tax preparers (both paid commercial and unpaid volunteer preparers) and about 60 million are prepared by consumers mostly using do-it-yourself tax software.

The security requirements for this community were first established by the FTC in 2003 pursuant to the FTC Safeguards Rule, which was issued under the authority of the Gramm-Leach-Bliley Act.

The current FTC Safeguards Rule provides for a relatively high level information security program for tax preparers serving consumers, which requires covered parties to: designate employee(s) to coordinate its security program; identify and assess risks to customer information and the effectiveness of current safeguards; design, implement, monitor and test an information security program, and adjust it according to relevant circumstances.[79]

Proposed changes to the Safeguards Rule will have a significant impact on tax preparers

On March 5, 2019 the FTC published a request for comment on proposed amendments to the FTC Safeguards Rule.[80]

Some of the proposed changes include:

- Requiring customer information to be encrypted, both in transit and at rest;

[79] See https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying#how

[80] https://www.ftc.gov/news-events/press-releases/2019/03/ftc-seeks-comment-proposed-amendments-safeguards-privacy-rules

- Requiring the implementation of multi-factor authentication for any individual accessing customer information;
- Requiring information systems to include audit trails designed to detect and respond to security events;
- Requiring the development of procedures for change management;
- Requiring the implementation of policies and procedures to monitor the activity of authorized users and detect unauthorized access or use of, or tampering with, customer information by such users;
- Requiring training and education, including verifying that key security personnel take steps to maintain current cybersecurity knowledge and using qualified security personnel; and,
- Expanding the requirement to oversee service providers to require the periodic assessment of such service providers based on the information security risk they present.

Selected sub-elements of certain additional proposed requirements would not apply to parties maintaining "customer information concerning fewer than five thousand customers" (although the remainder of such requirements would still apply to these smaller companies).[81]

Although there is clear recognition of the cybersecurity threat, there is not unanimity among the FTC Commissioners on the necessity for the proposed changes.[82]

However, it is clear that the proposed rule would set substantially more demanding requirements for the tax preparation community, large or small. This is particularly true for tax preparers (paid or volunteer), who generally are relatively unsophisticated in cybersecurity. A recent GAO report on third-party security reported opinions of industry preparer groups that preparers "did not know the steps that they should take to protect taxpayer information on their systems," and IRS officials reported that "paid preparers often do not know that they experienced a security incident until IRS informs them something is wrong with their filing patterns."[83]

The circumstances require that any amendments to the Safeguards Rule be accompanied by an overall implementation plan that includes outreach, guidance and assistance to affected communities.

In the case of tax preparers, the issuance of the proposed rule without such a plan could easily disrupt the tax preparation community leaving the IRS to bear the consequences.

---

[81] Elements of certain requirements that might be excluded for smaller companies fall in the areas of written risk assessments, testing and monitoring, and incident response plans. However, the interpretation and application of any exclusions will require additional analysis to understand their application in the tax preparation industry.

[82] See https://www.ftc.gov/system/files/documents/public_statements/1466705/reg_review_of_safeguards_rule_cmr_phillips_wilson_dissent.pdf.

[83] See GAO Third Party Cybersecurity Report, p. 17.

The IRS should engage with the FTC and tax preparation community on the proposed Safeguards Rule

Although the FTC has jurisdiction over the Safeguards Rule, the IRS is the federal agency that best understands the cybersecurity risks in the tax system and the capabilities and security of the tax preparation industry.

Given the significance of the proposed changes, the IRS should engage with the FTC and industry to understand the impact on the tax preparation industry including the substance of the proposed changes, industry's ability to comply with them and the type of support that industry may require to understand and implement the changes successfully.[84] This engagement is enabled by the study of tax preparer security practices and vulnerabilities recommended elsewhere in this Report.

The engagement between the IRS and FTC should also establish an ongoing mechanism for the agencies to review and discuss the effectiveness, enforcement and potential changes to the FTC Safeguards Rule as it may affect the tax preparation community.

……

Tax System Security

ISSUE: The end-to-end public and private tax system must be secure. To achieve that objective, the IRS must lead a coordinated effort to understand the risks to the tax system, and develop and execute an effective cybersecurity strategy. The IRS's success in this area also requires it to have clear authority and adequate funding, which has already been addressed in this Report (See Recommendation #4).

RECOMMENDATION #7: *Study information security practices and vulnerabilities in the tax preparer community*

As further outlined by ETAAC in this Report, the IRS should engage a qualified third party to conduct an initial study of the tax preparer community to understand its different segments and operating models, determine the state of its information security practices and vulnerabilities, and identify the range of high level strategic options and associated costs to remediate these risks.

Support for Recommendation:

Cybersecurity is the first line of defense against cybercrime and disruption

The first line of defense to cybercrime and disruption is robust cybersecurity.

[84] The study contemplated by ETAAC's 2020 Recommendation #7 would address these types of questions.

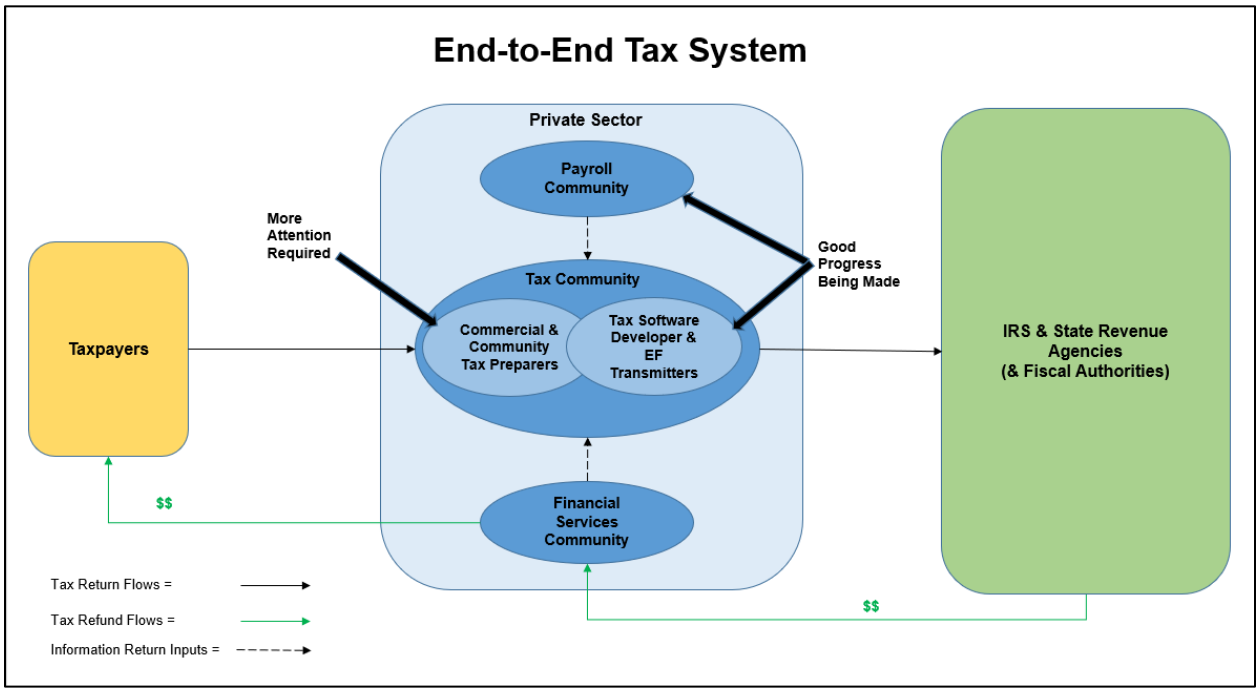
The GAO continues to identify cybersecurity as a high risk area, most recently noting that the effort to secure the nation's cyber infrastructure requires "especially focused executive and congressional attention."[85]

The Department Homeland Security (DHS) is responsible for securing federal networks outside of the defense and intelligence communities.[86] Numerous other federal agencies play a role in the cybersecurity area including: the Federal Bureau of Investigation (FBI), the National Institute of Standards and Technology (NIST), the Federal Trade Commission (FTC), the Federal Communications Commission (FCC) and the Small Business Administration (SBA).[87]

TIGTA has identified the security of taxpayer data and the protection of IRS resources as the top priority for IRS.[88]

The IRS recognizes this threat, and has correctly put a strong focus on the cybersecurity of its systems. The IRS Strategic Plan includes an objective to "safeguard taxpayer data and protect the IRS against internal and external threats," and the Modernization Plan identifies the protection of taxpayer information against cyber threats as a top priority.

Progress is being made to secure some tax segments, but more attention is needed on tax preparers



[85] See GAO High Risk Series Report (https://www.gao.gov/assets/700/697245.pdf).

[86] See https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

[87] See, for example: https://www.fbi.gov/investigate/cyber; https://www.nist.gov/topics/cybersecurity and https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity.

[88] TIGTA Management and Performance Challenges Facing the IRS for Fiscal Year 2020 (October 2019).

But the cybersecurity threat is not just to IRS systems – third-party tax systems are exposed as well.

The IRS has made a strong effort to improve third-party cybersecurity area in some key areas. For example, the Security Summit's Strategic Threat Assessment and Response (STAR) Work Group has made good progress to implement the NIST Cybersecurity Framework in the tax software area. STAR is also in the early stages of increased engagement with the representatives of the Payroll Community. And, regarding tax preparers, the IRS has implemented creative communications and education programs to increase cybersecurity awareness and provided some tools to assist them.

However, ETAAC believes that the security and vulnerability of tax preparers requires additional attention given their possession of high quality personal information being targeted by cybercriminals while, on average, being relatively unsophisticated in cybersecurity.[89]

Improving the cybersecurity of tax preparers will not be easy. In a recent report on the IRS's oversight of third-party cybersecurity, the GAO identified several issues concerning preparer oversight based on its discussions with officials from tax preparation groups and the IRS[90]:

- Most preparers, especially small firms or individual preparers, do not know the steps that they should take to protect taxpayer information on their systems.
- Preparers often do not know that they experienced a security incident until the IRS informs them something is wrong with their filing patterns.
- Preparers often have misconceptions as to what is required of them in protecting taxpayer data, e.g., industry group officials told GAO that the IRS's current publications are not clear about requirements versus leading practices.
- The imposition of standards for preparers, whether related to competency or information security, without explicit authority could leave the IRS vulnerable to legal challenges.

Any standards or requirements must be carefully targeted and not unnecessarily overwhelm the tax community

Importantly, the establishment of new standards does not necessarily require the introduction of new security standards, technical procedures or unnecessarily burdensome requirements such as IRS or third-party security audits. There are a variety of tools that the IRS could use to enhance cybersecurity in the tax preparation community. For example, requirements might focus on continuing security education, or the IRS might issue guidance on existing security standards as opposed to creating new standards. The IRS might also consider creating a voluntary security training program analogous to its current Annual Filing Season Program. The IRS's focus should be on

[89] In FY2019, IRS issued approximately 800,000 Preparer Tax Identification Numbers (PTINs). Additionally, IRS has approximately 300,000 Electronic Return Originators (EROs) under the Authorized IRS e-file Provider Program.

[90] See GAO Third Party Cybersecurity Report.

successfully improving tax preparer or ERO security, not merely piling on new regulations onto parties already overwhelmed by cybersecurity.[91]

It is misplaced to believe you can regulate your way into improved cybersecurity in this segment. IRS initiatives in this area should be targeted, phased and achievable -- trying to do too much too quickly could backfire. Any new compliance obligations should be part of a comprehensive, phased rollout that includes education and assistance. Additionally, any standards proposed by the IRS should be carefully tailored the address the level and types of risks presented. For example, an initiative to apply the NIST Cybersecurity Framework to individual tax preparers and small tax firms could easily overwhelm them and not result in any sustainable improvement in their security posture.

IRS should leverage the expertise, insights and content of other agencies

The IRS has an opportunity to leverage partnerships in this area. Several federal agencies (FTC, SBA, NIST, DHS, FCC, …) are engaged in industry-related cybersecurity. The IRS could extend its capabilities by working with other agencies, as well as the private sector, to leverage insights, content and expertise.

The IRS already does this to some extent, such as its promotion of the NIST publication "Small Business Information Security – The Fundamentals." But, there may be other opportunities to leverage content or expertise developed by these agencies, especially those targeted to small businesses. Unfortunately, to ETAAC's knowledge, no agency has yet formally assessed the best way to engage with small businesses to help them improve their cybersecurity.

IRS should commission a study of tax preparer information security to help identify its focus and options

The IRS is the best positioned federal agency to work with tax preparers to improve their cybersecurity. It has a deep understanding of their role in the tax system, the type of personal information they possess, the types of tax software they use and many of their other challenges. The IRS interacts with tax preparers on a daily basis and has established channels of communication. No other federal agency has this level of insights and connections.

At this time, however, the IRS is dealing with incomplete information concerning tax preparer security. It does not have a deep understanding of the state of tax preparer information security and their vulnerabilities, especially as it relates to the systems of electronic return originators (EROs).[92] ETAAC has had a continuing concern in this area, which has been raised in each of ETAAC's last three Reports.

---

[91] Existing federal cybersecurity resources provide excellent information but would likely overwhelm small businesses. See, for example, the DHS Small Business Roadmap (https://www.us-cert.gov/sites/default/files/c3vp/smb/DHS-SMB-Road-Map.pdf) and NIST Small Business Information Security (https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf).

[92] Under the IRS Authorized IRS e file Provider program, an ERO originates the electronic submission of returns it either prepares or collects from taxpayers who want to e-file their returns. See IRS Pub. 1345.

This current situation makes discussions in this area difficult, and contributes to the absence of a comprehensive, holistic strategy to engage with the ERO and tax preparer communities to improve their cybersecurity.

The conduct of a basic study of the tax preparer community to understand its security risks and vulnerabilities would not require additional statutory authority or significant funds. But, a study would greatly inform the discussion and deliberations on what to do in this area. ETAAC recommended such a study in 2019 and is, again, recommending this action.[93]

An initial study would accomplish several important objectives.

First, the study should evaluate and explain the various types of "tax preparers," e.g., individual income tax preparers (paid and volunteer), payroll tax companies, consumer tax software companies and professional tax software companies.

Second, the study should evaluate and explain different business models and structures among tax preparers. For example, the study should articulate how individual tax preparers are organized, e.g., firms vs. individual preparers. By way of illustration, the IRS reports an estimated 800,000 PTIN holders and approximately 330,000 EROs. The IRS must understand these numbers to know the scope of its challenge, e.g., there may be 330,000 ERO's but, from an organizational structure view, how many actual firms are there as opposed to multiple offices of a single firm.

Third, the study should identify preparer risks and challenges, and the potential options and their relative cost/benefit for a security oversight program.

Fourth, a study should clarify the existing authorities of the IRS to establish and enforce security standards.

Finally, such a study would inform Congressional oversight and appropriations discussions by identifying the potential scope of a program, its cost/benefit, required funding and needed authorities. It would also inform any discussions with the FTC concerning the impact of its proposed changes to the Safeguards Rule.

IRS-commissioned studies and GAO reviews have been invaluable in the past to help inform policy discussions, e.g., the IRS Advancing E-file Studies.[94] There is no reason why the same would not be the case in this instance.

III. IMPROVE THE TAXPAYER EXPERIENCE

INTRODUCTION

The recommendations in Part III focus on improving taxpayer services and the customer experience to enable compliance.

Recommendation #8 will help to ensure that taxpayers can access future IRS electronic services by encouraging the development of user-friendly and accessible digital identity

[93] ETAAC 2019 Report to Congress, Recommendation #6. (ETAAC is not aware of any significant action on this recommendation.)

[94] See https://www.irs.gov/e-file-providers/irs-advancing-e-file-study-key-messages.

solutions, which are the front door to these services. Recommendation #9 encourages the IRS to extend its taxpayer-controlled "real-time" protections that are commonly available elsewhere in our financial system. Recommendation #10 proposes that the IRS expand its collaboration on the design and launch of the IRS 1099 internet-based service required pursuant to the Taxpayer First Act. Finally, Recommendation #11 recognizes the opportunity to make it easier for the IRS to release legitimate business returns by increasing the accuracy of EIN responsible party information.

……

ISSUES & RECOMMENDATIONS

……

Digital Identity

ISSUE: Digital identity – the ability to remotely identity proof and authenticate persons -- is a critical dependency for the IRS's modernization strategy that enables improved taxpayer service and enforcement. ETAAC supports the IRS's collaborative approach to this area, and encourages the IRS to evaluate feasible methods to expand the availability of identity proofing options in non-digital channels. As recommended above, ETAAC believes that the development and implementation of digital identity solutions presents government-wide challenges that warrant Congressional attention and support.

RECOMMENDATION #8: *Collaborate on the identification and piloting of promising digital identity solutions*

The IRS should engage regularly with external subject matter experts, including Security Summit members, to identify and potentially pilot promising technologies or approaches to verify identities.

Support for Recommendations:

IRS electronic services require secure, accessible and compliant identity solutions

Recent ETAAC Reports have discussed the IRS's need to provide digital and mobile services to meet taxpayer and other stakeholder needs and expectations. Because many of these services cannot be provided without effective digital identity solutions, the IRS has prioritized digital identity initiatives as an element of the IRS Strategic Plan.

Digital identity is a very challenging area.[95] It is not enough to have a "secure" solution. It must also be usable by a high percentage of taxpayers, and flexible enough to be changed and refined over time based on situational developments.

[95] A recent TIGTA Report reviewed IRS progress in this area and some of the associated challenges. TIGTA Report: While Progress is Being Made on Digital Identity Requirements (March 23, 2020) (See https://www.treasury.gov/tigta/auditreports/2020reports/202020012fr.pdf).

However, no remote digital solution offers a silver bullet, and many taxpayers will still need access to a non-digital channel for identity proofing. For that reason, ETAAC continues to believe that the IRS must find ways to extend its physical footprint and consider the feasibility of creating trusted third-party identity proofing programs.[96]

The IRS is developing a new digital identity platform to replace its current "Secure Access" platform

Secure Access is the IRS's current digital identity platform that requires improvements to comply with newer technical and policy requirements.

The IRS is designing a next generation digital identity platform to meet these new requirements; namely, the Secure Access Digital Identity (SADI) platform.[97] SADI differs from Secure Access in several material ways. The biggest difference is that the SADI platform will be NIST 800-63-3 compliant. NIST 800-63-3 requires the IRS to validate and verify the identity evidence (i.e. driver's license or passport) provided at registration by checking specific features of the document and referencing the issuing source to confirm matching information. Individuals will also be asked to take a photo with liveness detection to match against the identity evidence.

Consistent with OMB M-19-17, SADI is being designed and built to leverage shared service Credential Service Providers, e.g., Login.gov and commercial providers. These service providers would verify public users (e.g., taxpayers) that access IRS applications and those of other agencies, which would improve the user experience and create government-wide efficiencies.

The IRS recognizes that implementing secure, usable digital identity solutions is a challenge that requires close collaboration with commercial and federal partners. The IRS is currently testing potential Credential Service Provider (CSP) solutions with external vendors. As part of this process, the IRS has met with commercial and federal (Login.gov) solution providers for product demos. Additionally, IRS executive participation at security conferences discussing digital identity solutions and development has led to further engagements between the IRS and federal entities and commercial companies working in this area. Moreover, the IRS is finalizing an Innovations Process to prioritize identity proofing, authentication and authorization studies that test potential solutions leveraging partnerships with both commercial providers and federal agencies.

ETAAC supports the IRS's collaborative approach. Security Summit state and industry experts are another source of collaborative partners who can both provide insights on technical solutions as well as offer deep insights into taxpayer accessibility and usability. They can also provide the IRS with insights into the most effective way to launch new solutions, and capture and apply learnings quickly.

---

[96] See 2019 ETAAC Report to Congress, Recommendation #8.

[97] Although not listed in the Modernization Plan, SADI provides foundational capabilities needed for access to services in the plan. The Commissioner approved SADI funding for FY2020 and FY2021 using user fees.

SADI enables implementation of key improvements to the taxpayer experience

The IRS's deployment of a compliant digital identity solution (i.e., SADI) has a direct effect on its ability to deliver key enabling technologies that drive better taxpayer experiences and IRS operating efficiencies. IRS activities to expand digital customer service and allow for electronic form submission are dependent upon the ability to authenticate that the signer is who they say they are.

IRS has been working on a plan to accelerate the use of electronic signatures under established federal standards.[98]

Because of the difficulty in finding commercial electronic signature solutions that meet the IRS's requirements (e.g., NIST compliant), the IRS has been developing an in-house e-Signature storage and retrieval service that can be integrated into applications. The storage and retrieval service is targeted for completion in the second half of 2020.

However, the outward facing capability for e-Signature must be built for a paper form to convert to a digital form that can be electronically signed and submitted to the IRS. This technology would also support the requirements of the Taxpayer First Act's Sections 2201 (Third Party Income Verification) and 2302 (Disclosures to Practitioners). Of course, the development of this capability is dependent on Congressional funding for e-Signature initiatives as part of the Modernization Plan.

As with SADI, the IRS's e-Signature implementation would benefit from its collaboration with states and industry, who can provide a perspective on taxpayer and tax professional needs and concerns, the prioritization of forms and applications, consumer and professional usability considerations, and security and authentication challenges

……

Taxpayer-Controlled Protections

ISSUE: In other areas of their financial lives, consumers are familiar with numerous account security features including proactive notifications and other controls. The IRS could make comparable protections available through individual and business taxpayer accounts to supplement its IP PIN Program.

RECOMMENDATION #9: ***Implement taxpayer-controlled "real-time" protections***

The IRS should continue to investigate, develop and implement proactive notification, lock/unlock and other taxpayer-controlled "real-time" protective features for individual and business taxpayer accounts.

[98] In December 2019, IRS issued an enterprise-wide policy for e-Signature usage, including minimum requirements around key areas such as the identification and authentication of the signer, validation of the intent to sign and forms of electronic form of signature. See Internal Revenue Manual (IRM) section 10.10.1. The IRM requirements are based on applicable law, NIST standards and other relevant guidance.

Support for Recommendation:

Consumers are very familiar with account notifications and controls

Millions of consumers are familiar with account notifications and controls.[99]

For example, several mechanisms (including "fraud alerts" and "security freezes") have been created to prevent identity thieves from accessing credit files to create bogus credit accounts in a legitimate consumer's name.

A fraud alert can be used by a consumer whose personal information has been misused or is otherwise concerned about possible identity theft, e.g., a wallet, Social Security card or other account information has been lost, stolen or exposed in a data breach. A fraud alert makes it harder for an identity thief to open accounts in your name because a business must verify your identity before it issues credit.[100]

Alternatively, a security freeze (sometimes called a credit freeze) restricts access to your credit report, which effectively locks your credit file thereby making it more difficult for identity thieves to open new accounts in your name.[101] Some credit reporting agencies have created online centers to manage security freezes.[102]

These types of protections are not unique to credit reporting agencies. Many banks provide the ability to create account settings to issue proactive notifications of log-ins or other activity such as withdrawals.

Currently, the IP PIN is the IRS's principal IDTTRF prevention tool for taxpayers

The IRS does not provide an option for a taxpayer to receive notifications about tax account activity (such as a transcript request or return filing) or to "lock" their taxpayer account to prevent a tax filing in their name.

The only proactive IDTTRF-related solution is the IRS's Identity Protection Personal Identification Number (IP PIN), which the taxpayer must apply for and include with the filed return. The return will not be accepted for filing with the IRS without the IP PIN. In the past, the IP PIN has only been available to confirmed victims of identity theft. Now, however, the IRS is in the process of a phased implementation to make the IP PIN available to any taxpayer who wants one. For 2020, a taxpayer from any of 20 states is eligible for the online IP PIN Opt-In Program.[103] Over the next few years, the IRS will expand the availability of the IP PIN Opt-In Program nationwide.

However, the IP PIN presents its own complexities. It must be obtained in advance and included for any taxpayers or dependents on the tax return who have an IP PIN. A new IP PIN must also be distributed each year.

---

[99] For example, an estimated 1 in 5 Americans froze their credit with one or more of the big three credit bureaus after the Equifax breach. See https://www.equifaxsecurity2017.com/2017/09/07/equifax-announces-cybersecurity-incident-involving-consumer-information/ and https://www.fundera.com/resources/credit-freeze-after-equifax-breach.

[100] See https://www.consumer.ftc.gov/articles/0275-place-fraud-alert.

[101] See https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs#what.

[102] See Experian's "Security Freeze Center" (https://www.experian.com/freeze/center.html).

[103] See https://www.irs.gov/pub/irs-pdf/p5367es.pdf

There are several options to provide additional proactive protections to taxpayers

Other real time options could be provided to supplement the IP PIN. The IRS is evaluating a number of them including:

- Push Notifications: Taxpayers receive notices on their IRS2Go App of specific activities concerning their account, e.g., Modernized e-File System (MeF) filings, transcript requests or third-party access of their account.
- MeF Filing Lock: Taxpayers control when an electronic return is filed for their account.
- Transcript Lock: Taxpayers control when a third party can request transcripts of their accounts (e.g. IVES, FAFSA).
- Preparer Access: Preparers can unlock a taxpayer's account for a designated period to file a tax return
- Dependent Account Lock: Primary taxpayer has ability to stop all returns filed using their spouse or dependents as a primary taxpayer

Account notifications, controls and lock/unlock features should be additional options for taxpayers

The IP PIN solution is certainly one approach to help block IDTTRF filings. However, taxpayers have increased expectations and should have more options to protect themselves.

In 2018, ETAAC supported the IRS's investigation and development of lock/unlock features for individual and business taxpayer accounts.[104]

ETAAC continues to believe that notification, lock/unlock and other taxpayer-controlled "real-time" protective features for individual and business taxpayer accounts warrant the IRS's continued investigation, development and implementation.

……

Form 1099 Internet Filing Platform

ISSUE: Section 2102 of the Taxpayer First Act requires the IRS to make available an Internet platform or similar service that allows persons to prepare, file and distribute Forms 1099 and maintain a record of completed, filed, and distributed Forms 1099.

RECOMMENDATION #10: *Expand collaboration on the design and launch of the IRS 1099 internet-based service*

The IRS should expand its existing collaboration with states and industry in the design and implementation of the TFA-mandated 1099 service in a way that anticipates its integration into future modernized IRS systems.

[104] See 2018 ETAAC Report to Congress, Recommendation #18.

Support for Recommendation:

The IRS Fire System is being supplemented by a new IRS Form 1099 filing platform

An information return is a tax document used to report certain types of payments made by financial institutions and others who make payments as part of their trade or business. Information returns include Forms 1099, 1042-S, 1097, 1098, 3921, 3922, 5498, 8027, 8955-SSA, and W-2G, which may be filed electronically using the Filing Information Returns Electronically (FIRE) System.

Every year, various issuers or payers (e.g., corporations, partnerships, trusts, non-profits, individuals, or government entities) file over 3 billion Form 1099 information returns with the IRS to report specified transactions.[105] The most common Form 1099's include 1099-B, 1099-INT, 1099-DIV, 1099-MISC, 1099-R and 1099-G.

As a supplement to other IRS services, TFA Section 2102 requires the IRS to make available by January 1, 2023 a secure platform[106] for Form 1099 filings to: prepare and file Forms 1099; prepare Forms 1099 for distribution to recipients other than the IRS; and, maintain a record of completed, filed, and distributed Forms 1099.

IRS's implementation of the new 1099 internet platform would benefit from a collaborative approach

In its implementation of the Taxpayer First Act Section 2102, the IRS has been conducting outreach to external stakeholders, including IRS' advisory groups, representatives of payroll and similar industry groups that provide commercial Form 1099 preparation and submission services, and state and other government agencies that have systems for Form 1099 (or equivalent) information return preparation and submission. The IRS is using insights gained from outreach to identify best practices, to inform system requirements and design, and to understand what functionality is important to potential users of the new system.

ETAAC believes that the IRS should continue its collaboration with states and industry on the design of this 1099 filing service. This approach would help the IRS avoid developing a stove-piped or silo'ed solution, such as the service to upload ACA-related Forms 1094/1095. Instead, the new 1099 service should contemplate full integration into the broader future IRS IT architecture and services in a manner to enable data to flow between other related or dependent applications.

The new 1099 system might also be designed to enable real-time data validation between the IRS and states. Currently, there is a long delay before the states receive 1099 filing information from the IRS. The IRS should consider whether the new 1099

[105] See TIGTA Report "Strengthened Validation Controls Are Needed to Protect Against Unauthorized Filing and Input of Fraudulent Information Returns" (Sept 29, 2019).
https://www.treasury.gov/tigta/auditreports/2019reports/201940071fr.pdf

[106] The TFA specifies an "internet website or other electronic media, with a user interface and functionality similar to the Business Services Online Suite of Services provided by the Social Security Administration."

platform could support real-time validation of 1099 filing information by states to help identify compliance or IDTTRF issues.

By way of illustration, imagine that a criminal steals a dormant business identity to submit 1099's with federal and state withholdings (but makes no withholding payments). After filing false 1099s, the criminal then files individual income tax returns for all 1099 recipients to claim refunds of withholdings. An integrated 1099 platform could be designed to alert the IRS that 1099's were received from a dormant taxpayer (no other active tax filings on record, e.g., 990, 1120, 1065. 1040 Schedule C or 94x payroll reports), which could then trigger an alert on all recipient accounts.

……

Employer Identification Numbers

ISSUE: The accuracy and integrity of "responsible party" information associated with an Employer Identification Number (EIN) is essential to resolving potential IDTTRF returns. When this information is out of date, legitimate taxpayers are disadvantaged when the proper handling of suspect (but legitimate) returns is delayed.

RECOMMENDATION #11: ***Increase accuracy of EIN responsible party information***

The IRS should review current EIN-related processes with Security Summit and other external stakeholders to obtain recommendations to increase awareness of and compliance with the EIN holder's obligation to report changes in its responsible party.

Support for Recommendation:

The "responsible party" under an EIN plays a critical role in the prevention of business IDTTRF

An EIN, sometimes referred to as a Federal Tax Identification Number, is a numeric identifier for a business tax filer. In effect, it is the business filer equivalent of a social security number for an individual filer.

EIN applications require the name and Taxpayer Identification Number of the "responsible party" for the business. The responsible party is the person who ultimately owns or controls the entity or who exercises ultimate effective control over the entity. Unless the applicant is a government entity, the responsible party must be an individual (i.e., a natural person) not an entity.

Pursuant to IRS regulations effective January 2014, an entity with an EIN is required to report a change in its responsible party within 60 days by filing IRS Form 8822-B.[107] These types of changes can occur when, for example, a person dies, changes

[107] 26 CFR § 301.6109-1 Identifying Numbers.

employment, terminates an officer position with a business or transfers his or her ownership interest in a business.

Responsible party information is not being updated by EIN holders – that is a problem

The identity of the responsible official is critical in situations where IDTTRF is suspected in connection with a business return. The IRS will try to contact the business entity and the associated responsible party. Outdated or inaccurate responsible party information adversely impacts the IRS's investigation of the return, particularly in the case of a fraudulent return where the address has been changed. Inaccurate entity information also makes the entity vulnerable. Specifically, a person no longer associated with the business but still listed as the responsible party with the IRS has the authority to obtain information and make changes to the account.

This situation presents a problem for the business taxpayer because the IRS will suspend the processing of a suspect return until it can be verified. The IRS attempts to send a letter to both the business and responsible party's address of record to verify the legitimacy of the return which, of course, will not be received without accurate information. The return will remain unprocessed which can result in refund delays, offsets and penalties.

Several years ago, the IRS began requesting that the signer of the return voluntarily provide his/her full name and TIN in the return schema so as to identify the responsible party. In the future, the IRS expects to provide an alert back to the software companies for those returns that do not have this information. In the future, the IRS may require that this information be provided.

The requirement to update responsible party information is relatively new – just over five years old. Although there is a requirement to update responsible party information, there is no penalty for a failure to do so. Additionally, there is no impact on the filing of a business tax return, which does not require the identification of the responsible person on the tax form.

There are opportunities to increase awareness of the updating requirement

ETAAC has identified several potential opportunities to increase EIN holder awareness of the need to or importance of notifying the IRS of any changes in the responsible party, including:

- The Form SS-4 (Application for Employer Identification Number) should indicate the necessity to update the IRS in the event of a change in responsible party information.
- Although the Instructions for Form SS-4 include a "Tip" that states "File Form 8822-B to report any subsequent changes to responsible party information," it does not mention the 60 day filing requirement.
- The EIN issuance confirmation letter from the IRS could notify EIN holders about the need to update the IRS on changes in responsible party, e.g., adding this point as an "Important Reminder" on the letter templates.

- Adding or increasing information on IRS.gov concerning this requirement.

There are clear opportunities to increase awareness of the requirement well short of fining EIN holders for failing to timely update information.

First, the IRS can be more proactive and prominent in communicating the requirement on its forms, on IRS.gov and in other taxpayer communications.

Second, in the tax space, the IRS can engage key stakeholder communities to increase the awareness of their customers who may be EIN holders, e.g., tax and payroll software companies, service providers, tax professionals, etc.

Third, there may be other touchpoints to engage with EIN holders to solicit updated information, such as at the time of filing a tax return.

Fourth, beyond the currency of information, there may be other gaps. For example, the SS-4 only requires the name and tax identification number of the responsible party but not their contact information. The business' contact information may be different than that of the responsible party.[108]

Finally, it does not appear that business and employment tax returns require the identity of the responsible party. If they did, there might be an opportunity for the IRS to match the responsible party identified on the return with the person identified in the IRS's records for the EIN holder.

In conclusion, ETAAC believes that the appropriate action is for the IRS to collaborate with Security Summit members and other external stakeholders to identify options to increase awareness of, and compliance with, the obligation of EIN holders to update changes in the responsible party in a timely manner.

IV. STRENGTHEN THE SECURITY SUMMIT & ISAC

INTRODUCTION

The recommendations in Part IV focus on strengthening the Security Summit and ISAC.

Recommendation 12 would ensure that the IRS redesign effort required by the Taxpayer First Act (TFA) contemplates the Security Summit, and uses that opportunity to review opportunities to strengthen the Summit. Recommendations 13 – 15 focus on ISAC-related opportunities to implement certain TFA provisions, mitigate risks posed by ISAC personnel turnover, and provide more structured training to improve ISAC participant performance. Finally, Recommendation #16 supports the IRS's efforts to implement real-time EFIN and PTIN validation capabilities.

……

ISSUES & RECOMMENDATIONS

……

[108] Federal and state EIN information may also provide insights in the ISAC if that information were shared.

Security Summit

ISSUE: Since its creation in 2015, the IRS Security Summit has contributed significantly to reducing and preventing identity theft tax refund fraud (IDTTRF) in the individual income tax area.[109] Pursuant to the TFA, the Treasury Department is required to develop a comprehensive plan to redesign the organization of the IRS. The TFA also requires the IRS to work collaboratively with the public and private sectors to protect taxpayers from IDTTRF. The IDTTRF battle is not over, and the Security Summit must remain vigilant to sustain its past success. In connection with any redesign, the IRS should assess and address the impact of any new structure on the Security Summit. Such an assessment should, as well, ensure that the Security Summit's structure, management, goals, priorities and operation can sustain its success and the commitment of its partners.

RECOMMENDATION #12: *Evaluate TFA impact on Security Summit and sustain energy and commitment of participants*

The IRS should work with the Security Summit's state and industry leadership to evaluate the impact of any IRS organizational redesign pursuant to the Taxpayer First Act on the Security Summit's structure and operations, and to identify and act on specific opportunities to drive and sustain the Summit's effectiveness, efficiency and participant energy and commitment.

Support for Recommendation

IDTTRF presented a significant and rapidly growing threat in 2015 – the Security Summit has responded successfully

The IRS was faced with an unambiguous challenge in 2015 as cybercriminals were stealing billions of dollars in fraudulently obtained individual income tax refunds.[110]

The IRS Commissioner took a public leadership role in calling together leaders from state revenue departments and private sector tax-related service companies to discuss the challenge and solicit ideas on how to collaborate on possible solutions. The subsequent outcome was the establishment of the IRS Security Summit in March, 2015. The IRS, states and industry committed expert resources to the effort, key areas were identified and working groups around them organized. These groups developed and began executing effective action plans, and success in mitigating IDTTRF followed.

Preventing IDTTRF is a strategic priority for Treasury and the IRS

Preventing IDTTRF remains a top priority for the Treasury Department and the IRS. This area is one of only three Treasury Department FY2020 – 2021 Agency Priority

[109] The Security Summit currently consists of six Work Groups (Authentication, Information Sharing, STAR, Communications and Taxpayer Awareness, Financial Services and Tax Professional) and the ISAC.

[110] GAO reported that, in 2014 alone, the IRS estimated that it had paid out $3.1 billion dollars in IDTTRF refunds (See https://www.gao.gov/assets/680/677406.pdf).

Goals, and the only one for the IRS.[111] The importance of this area is reinforced by TIGTA, which views preventing IDTTRF among the IRS's top three management challenges preceded only by cybersecurity and tax law implementation.

The opening page of the IRS Strategic Plan notes its focus on "combating the increased prevalence of refund fraud and identity theft," elements of which are incorporated into several strategic goals including collaborating with external partners, using advanced data access and analytics and driving increased security in IRS operations.

The momentum and success of the Security Summit relies on several key contributing factors

Several key factors have created the Security Summit's focus, commitment and energy including:

- A clear, articulated IDTTRF threat
- Strong top down leadership, commitment and support from the IRS, states and industry
- Broad perspectives from IRS, state and industry participation
- Deep expertise of individual contributors in key areas, e.g., fraud, cybersecurity and technology
- An established structure, governance model and supporting policies that drive innovation and accountability
- Trust & collaboration based on open communications and working together to solve tough government and private sector challenges

The leadership of the Security Summit must reinforce these factors on a continuing basis to sustain the commitment to and success of the Security Summit.

Despite its success, the Security Summit must maintain a constant and focused vigilance.

As evidenced above, individual income tax IDTTRF has been considerably reduced from several billion dollars in annual losses to a few hundred million dollars (although individual tax IDTTRF attempts exceed $6 billion annually). Granted, this is much less than when the Security Summit first started. However, there is a danger of reversing this trend if, for some reason, the Security Summit inadvertently became less of an agency priority or if it lost state and industry support.

The Taxpayer First Act mandates the IRS redesign its organization to, among other things, implement the provisions of the TFA, streamline the structure of the agency including minimizing the duplication of services and responsibilities within the agency, and best position the Internal Revenue Service to combat cybersecurity and other threats to the Internal Revenue Service. ETAAC previously provided the IRS TFA

[111] See https://www.performance.gov/treasury/. For the most recent priority action plan, see https://www.performance.gov/treasury/2019_dec_Treasury_Fraud_Prevention.pdf, which includes several references the critical role played by the Security Summit.

Program Office with its observations of potential organizational duplication or gaps concerning cybersecurity and other disruptive threats (See Appendix D).

Additionally, any IRS restructuring could affect the operation of the Security Summit if critical IRS leadership were shifted from current Security Summit responsibilities. ETAAC has already observed that the continuity of Security Summit operations are affected when key leadership executives are no longer involved in the Security Summit. While this challenge is relevant to changes in both government and private sector leadership, the IRS sets the Summit's tone and direction and, therefore, its pivots can be more impactful.

The Security Summit's success, coupled with the inevitable personnel turnover effected by TFA's mandates, create the opportunity for a perception of "mission accomplished." The mission is, of course, not accomplished and any loss of focus or perspective, unintended or not, could exacerbate the risk of not staying vigilant while criminals simply retool.

As a reminder of the required vigilance, IDTTRF-related crime continues to evolve.

Sophisticated IDTTRF cybercriminals continue to see the IDTTRF financial opportunity as evidenced by over $6 billion in attempted individual tax IDTTRF filings. Just as important, adversaries may see the opportunity to disrupt the nation's tax system and economy.

These actors have the resources, technology and tax skills to find new ways to obtain taxpayer information to file false tax returns and claim fraudulent refunds. For example, identity thieves continue to target tax professionals, businesses, human resources departments and other sources of large amounts of sensitive personal and financial information.

In addition to sophisticated and well-funded adversaries, some of the other continuing or emerging IDTTRF-related threats include:

- Increasing threats to the business tax area where the IRS knows less about associated schemes
- Limited cybersecurity capability in small business communities, including tax professionals
- Increased cybercriminal targeting of high quality data sources, such as tax professionals, that will make it increasingly difficult for the IRS to distinguish legitimate and illegitimate returns
- A potential expansion of adversary objectives beyond just monetary gain to include the disruption of our US tax system and economy

The Security Summit serves a critical interest and, in light of the IRS's organizational mandates under the TFA, would benefit by using this opportunity to review its current structure and operations

In connection with the IRS's TFA organizational design review, the Security Summit, under IRS leadership, should step back and review its performance and how it can best maintain its current high level of member interest and resource commitments.

That review should have a particular focus on elements that strengthen or weaken the key factors (noted above) that have led to the Security Summit's success, in addition to ensuring the Security Summit receives priority and is aligned with the TFA. The review should focus on both IDTTRF prevention and cybersecurity, and involve considerations such as organizational roles and goals, operating mechanisms (e.g., meetings, reports, etc.), what's working, what's not working and what work groups or activities could be realigned, eliminated or consolidated to free up capacity to focus on higher priority Security Summit initiatives and activities or to avoid duplication of effort.

Such a review would provide an opportunity to consider several important questions:

- How can stakeholders best communicate and align on the Security Summit's strategy, goals and priorities.
- Are there opportunities to finetune the operational structures of the Work Groups or the ISAC?
- Can the operating mechanisms that drive Security Summit activities and progress be improved, e.g., meeting structure and cadence, member engagement, face-to-face vs. telephonic engagements, etc.?
- How can the IRS mitigate the impact of turnover in the Security Summit and its supporting organizations to ensure continuity, insights, energy, and relationships?
- What is the most effective way to build team capabilities and drive progress, e.g., targeted face-to-face working sessions or, conversely, applying new learnings about the conduct of virtual meetings via video conferences?
- What is the best way to communicate the progress of the Security Summit?
- How can the IRS best garner and sustain strong "top down" interest in and support for the Security Summit from stakeholder communities?

……

Information Sharing and Analysis Center (ISAC)

ISSUE: The ISAC is a key contributor to IDTTRF prevention. Several provisions of the Taxpayer First Act positively impact the operation of the ISAC, including key amendments to IRC Section 6103 to permit carefully limited disclosures of federal tax information to prevent IDTTRF. As the ISAC matures, it is important to identify opportunities to improve its performance. In that regard, ETAAC notes that state and industry ISAC participants are experiencing turnover which, if not handled effectively, can create inefficiencies and slow progress as new persons get up to speed on ISAC

policies, processes, operations and systems to detect and prevent IDTTRF. ETAAC believes there are opportunities to improve access to relevant information and to provide more systematic training programs to alleviate the impact of participant turnover and accelerate their contributions.

RECOMMENDATION #13: *Collaborate with State and Industry ISAC participants to implement TFA's ISAC-related provisions*

The IRS should collaborate with states and industry to develop and implement Section 2003 (b) and (c) of the Taxpayer First Act regarding ISAC performance metrics, information sharing agreements and related policies and procedures.

RECOMMENDATION #14: *Implement a structured on-boarding process to mitigate the adverse impact of continuing ISAC turnover*

The IRS should enable the ISAC Trusted Third Party to develop an on-boarding process including a review of ISAC reference and operational materials to mitigate the adverse impact of IRS, state and industry personnel turnover and accelerate the value provided by and to new ISAC participants.

RECOMMENDATION #15: *Implement a more structured training program to improve ISAC participant performance*

The IRS should enable the ISAC Trusted Third Party to implement a more structured approach for the development and delivery of ISAC platform training.

Support for Recommendation:

IRS's implementation of the Taxpayer First Act ISAC-provisions can be improved with collaboration

Information sharing enables the IRS, states and industry to detect and prevent IDTTRF. The primary platform for information exchange is the ISAC, which launched as a pilot in 2017 and became fully operational in 2018.

The Taxpayer First Act (TFA) statutorily formalizes the ISAC's role in centralizing, standardizing, and enhancing data compilation and analysis to facilitate sharing actionable information to prevent IDTTRF. ETAAC believes that the development and implementation of two key ISAC-related TFA provisions would be enhanced through the IRS's collaboration with states and industry; namely, ISAC performance metrics pursuant to TFA Sec. 2003 (b), and "Information sharing agreements" and related IRS policies and procedures to implement the amendments to IRC 6103(k) pursuant to TFA Sec. 2003(c).

ISAC's performance can also be improved by anticipating and responding to participant turnover

ISAC Participants: Senior Executive Board, Trusted Third Party and Analysts Community of Practice

Participants in the ISAC contribute in two principal areas – ISAC management and ISAC operations.

At the strategic level, the ISAC partnership of the IRS, states and industry is managed by its Senior Executive Board (SEB), which has equal representation of executive-level leaders from each of its three stakeholder sectors. At the operational level, the ISAC has two key components – the Executive Official[112] and the Trusted Third Party (TTP).

The TTP performs a number of functions including: receiving and analyzing data from ISAC participants and other sources; providing anonymized, aggregated reports and visualizations to help members to better detect and stop IDTTRF; providing the secure platform to help users quickly find significant data anomalies; and, supporting users to help maximize the benefits of ISAC tools and analytic products.

The IRS should be commended for its recent decision to leverage the TTP to enhance program management and administrative support resources for the ISAC. This enhancement has already made a significant improvement in ISAC management, and will provide the stability and sustainability that the ISAC needs to ensure long term engagement and effectiveness. In exchange for this support, industry has agreed to support and organize the annual ISAC summer roundtable, which convenes Security Summit leaders, ISAC members and other government/academic/industry cyber experts to evolve the thinking and future focus of the ISAC.

The ACoP consists of a highly engaged body of front-line analysts from the IRS, states, and industry. The ACoP community enables these analysts to share and discuss ideas, knowledge, best practices and concerns about IDTTRF. It is led by a steering committee comprised of equal membership from each of the ISAC's three sectors and, organizationally, functions as a subcommittee of the SEB.

Participant turnover creates risks for the ISAC

Consistent participation by members of all sectors was experienced during the first years of the ISAC program. These individuals were in the front lines of designing, forming and implementing the ISAC, and developed a deep knowledge of the ISAC's issues, decisions and foundation.

Understandably, new members join the ISAC over time as existing individual participants depart for a variety of reasons – particularly at the analyst level. This turnover creates risk for the ISAC as new participants lack first hand familiarity of ISAC history, focus, mission and operations. Without that context, the ISAC's progress and operations are slowed as new people get up to speed.

[112] The Executive Official also works to ensure the SEB, TTP and ancillary teams remain in scope and funding levels.

To accelerate the effectiveness of new members, especially new leaders and Senior Executive Board members, the IRS should provide the resources to develop and implement an on-boarding and orientation experience for new members that would educate them on the resources and materials available on the platform and share the expectations and responsibilities of their new role. The orientation should include an overview of documents such as: signed participant agreements and amendments; policies and forms; meeting agendas, minutes and materials; training materials; presentations; webinars; metric reports; and annual reports. The TTP would be a logical choice to implement this action.

ISAC performance can also be enhanced through improved training

Leads[113] and alerts[114] are submitted by individual ISAC participants into ISAC's secure platform, and play a key role in bolstering IRS and State IDTTRF detection and prevention. Training is required to help new analysts use them effectively.

Currently, ISAC participant training is an opportunity for improvement. For example, the TTP provides some training, as do endorsing organizations such as the Federation of Tax Administrators (FTA). However, there is no structured approach for all participants to learn about and use these materials.

ETAAC believes that a more systematic approach to participant training would increase the effectiveness of all participants. First, the training materials should be consolidated and available in one place. Second, there may be other training topics and platforms that could be developed, e.g., on-line training modules for self-directed learning, periodic webinar training, and facilitated in-person training sessions in partnership with ISAC endorsing organizations. A progression of training that included recognition, such as establishing levels of mastery, would help motivate and recognize individuals who took the initiative to develop their skills and could serve as a mechanism to provide access to future advanced capabilities or access in the platform

……

Electronic Filing & Preparer Tax Identification Numbers

ISSUE: The accuracy and integrity of Electronic Filing Identification Number (EFIN) and Preparer Tax Identification Number (PTIN) holder information contributes to preventing and resolving IDTTRF issues. Realtime access enables states and industry to verify the legitimacy of EFIN and PTIN holders quickly and efficiently.

[113] Leads are collections of data from filed returns with potentially suspicious attributes that, when cumulated and analyzed with lead information from other ISAC participants, can help to illuminate more comprehensive cyber threats across our tax system.

[114] Alerts report IDTTRF threats, including immediate reports of breaches, compromised information or other suspect data. Exponential value is gained when ISAC participants build on alerts submitted by others. A more robust picture of IDTTRF is developed as more participants provide supplemental information associated with a given alert.

RECOMMENDATION #16: *Implement real-time EFIN and PTIN validation capabilities*

The IRS should continue to develop and implement a system to enable real-time electronic EFIN validation by authorized third parties and, once launched and operating effectively, evaluate options to extend this functionality to real-time electronic PTIN validation.

Support for Recommendation:

EFINs & PTINs are important in identifying and validating EROs and preparers

An Electronic Filing Identification Number (EFIN) is issued by the IRS in connection with the IRS e-file Program. Any tax return preparer expecting to file eleven or more Form 1040/1041 returns must e-file them. In order to e-file returns, the returns must be transmitted through an Authorized IRS e-file Provider (Provider), which is a business or organization (firm) accepted by the IRS to participate in the Program. The responsible official of the firm must submit an e-file application, meet certain eligibility criteria and pass a suitability check before the IRS will assign an EFIN, which must be included with all electronic return data transmitted to the IRS.

A Preparer Tax Identification Numbers (PTIN) is a number issued by the IRS to paid tax return preparers. Obtaining a PTIN requires that the preparer verify his or her identity with the IRS. The PTIN identifies the preparer and, when applicable, must be placed in the paid preparer section of a tax return.

EFINs & PTINs play a role in the fight against fraudulent and improper activity

Unfortunately, EFINs can be used improperly. In more benign settings, preparers not formally affiliated with an EFIN might use or "share" an EFIN to transmit legitimate returns, i.e., an unauthorized use of the EFIN. On the other hand, EFINs can be compromised and used to file fraudulent tax returns.

Within the IRS, a compromised EFIN could be identified in various ways -- a criminal investigation, a preparer audit or IDTTRF analytical processes. Outside of the IRS, a transmitter or ERO could identify a misuse by comparing the number of returns reported on its e-services account with the number of returns it knows have been filed from its offices (an indication that someone else has been filing returns under their EFIN).

Once identified, EFIN anomalies must be researched, confirmed and addressed. If an EFIN is determined to be compromised, IRS Electronic Products and Services Support (EPSS) will attempt to contact the firm, inactivate the EFIN, issue a new EFIN and notify the firm. EPSS will also review the situation to determine if further action is necessary, such as a fraud referral.

In advance of filing a fraudulent return, criminals possessing a compromised EFIN may try to license professional tax software.[115] To stop this type of scheme, tax software

[115] Professional tax software is designed to prepare, queue and e-file large volumes of returns.

companies currently conduct a manual process to collect information and documentation from potential customers to confirm they have legitimate EFINs.

The IRS is currently deploying the final stage of its EFIN verification process. This process will allow tax software providers to verify EFIN information provided at the time of software purchase and prior to each subsequent filing season with data held by the IRS.

Similarly, PTINs can be misappropriated and misused. Firms that hire preparers must be able to ensure any potential employees have valid PTINs because of the sensitive information they handle. It is one more step an employer can take to ensure the integrity of their firm because of the IRS's due diligence before issuing a PTIN.

ETAAC supports the IRS's current effort to provide a system that enables real-time EFIN validation

Both the IRS and industry acknowledge that protecting the integrity of EFINs and PTINs is important to IDTTRF prevention and the effective operation of our tax system. The limitations of the current "manual" processes to accomplish these validations are well known.

Fortunately, the IRS is well along on the effort to have a mid-year launch of a new EFIN validation system. The new system will be more streamlined, faster and more efficient than the current process. In connection with that deployment, the IRS is also working on a communication plan, a user guide and instructions, and other materials.

Additionally, there are opportunities to enhance IDTTRF prevention by scaling the EFIN solution to allow for verification of PTINs as well. This would strengthen the validation program to allow for additional protection against preparer-related IDTTRF.

Once the EFIN system is in place and operating, the IRS should consider its options to extend this functionality to real-time PTIN validation.

ELECTRONIC TAX ADMINISTRATION & PROGRESS TOWARD 80% E-FILE GOAL

COVID-19 pandemic impact on electronic filing

Several events during the 2020 tax filing season are impacting the volume and timing of tax return filings and associated payments.

Key events & actions

First, in response to the COVID-19 pandemic, the Treasury Department announced on March 21, 2020, the extension of the federal income tax filing due date for individuals, trusts and corporations from April 15 to July 15, 2020.[116] Tax payments due during this time frame were also deferred until July 15. Although taxpayers were not required to take any action to effect these delays, the IRS encouraged taxpayers expecting a refund to file their returns as quickly as possible.

Second, the Coronavirus, Aid, Relief and Economic Security Act (CARES Act) allows employers, with no special election, to delay the filing of quarterly Form 941s and the payment of related payroll taxes.[117]

Third, the CARES Act provided for Economic Impact Payments (EIPs) to qualifying taxpayers, which included $1,200 direct payments to taxpayers and their spouses and a $500 payment for each qualifing child. For these payments, the CARES Act required the IRS to use direct deposit information available from either the taxpayer's 2019 or 2018 tax return or, for social security or railroad retirement beneficiaries with no income tax filing requirement (so called non-filers), information from the Social Security Administration.[118] All other EIP recipients would receive a paper check from the IRS.

IRS and Industry worked together quickly to help taxpayers

The IRS with the support of the tax industry took several actions to accelerate the delivery of EIPs to non-filers via direct deposit.

The IRS enaged with the Free File Alliance to have the Alliance develop a website in less than a week that enables non-filers to submit relevant payment and other required information to the IRS to enable direct deposit of EIPs (Non-Filer Tool).[119] That non-filer tool is available to taxpayers through the IRS web site.[120]

As a supplement to the Non-Filer Tool, the IRS also authorized the creation and filing of a "simplified return" by individuals with zero AGI or who otherwise did not have a filing requirment due to income limitations.[121] Several commerical software providers have created and are providing services to enable taxpayers to file these simplified returns.

---

[116] IRS News Release IR-2020-58, March 21, 2020 (https://www.irs.gov/newsroom/tax-day-now-july-15-treasury-irs-extend-filing-deadline-and-federal-tax-payments-regardless-of-amount-owed).

[117] See https://www.irs.gov/newsroom/deferral-of-employment-tax-deposits-and-payments-through-december-31-2020.

[118] IRS later added SSI and VA recipients to direct deposit.

[119] See https://www.irs.gov/newsroom/treasury-irs-launch-new-tool-to-help-non-filers-register-for-economic-impact-payments.

[120] See https://www.irs.gov/coronavirus/non-filers-enter-payment-info-here.

[121] See IRS Revenue Procedure 2020-28. See https://www.irs.gov/pub/irs-drop/rp-20-28.pdf.

Additionally, industry provided the IRS with feedback on EIP execution, while acting as a communications channel for the IRS to distribute information to taxpayers concerning EIPs.

ETAAC wants to recognize this cooperative effort to serve the taxpayer during these unprecedented times. It required an effective working relationship to respond quickly in a rapidly shifting environment to communicate and execute contingency plans to deal with changes in tax due dates, penalties and credits and, at the same time, deliver economic impact payments. That working relationship enabled taxpayers to continue to submit their taxes and receive their refunds and EIPs notwithstanding a global pandemic. Bottom line – the tax system worked.

Measuring Progress Towards The 80% Electronic Filing Goal

Congressional targets

Section 2001(a) of the IRS Restructuring and Reform Act of 1998 (RRA 98)[122] provided that "It is the policy of Congress that -- paperless filing should be the preferred and most convenient means of filing Federal tax and information returns; it should be the goal of the Internal Revenue Service to have at least 80 percent of all such returns filed electronically by the year 2007; and the Internal Revenue Service should cooperate with and encourage the private sector by encouraging competition to increase electronic filing of such returns." Section 2001(b)(2) of the RRA 98 authorized the creation of the ETAAC, whose charter provides that it will research, analyze, consider and make recommendations on the IRS's progress toward achieving its 80% e-file goal.

The IRS interpreted the RRA 98's 80% goal to apply to "major returns,"[123] and ETAAC has generally followed this approach in reviewing the IRS's progress towards the 80% goal for the purposes of the ETAAC's Annual Reports to Congress.[124] (Also see Appendix E)

2020 filing season

The full impact of the COVID-19 response on tax return volumes and electronic filing is currently unknown.

As of April 10, 2020, the IRS reported that it had received approximately 15.5 million fewer returns as compared to the comparable prior year period – a decline of about 13%. Of course, given the deadline delay, this insight is not surprising and additional insights will be developed during the rest of the filing season. ETAAC would expect the e-file rate to normalize as the IRS gets closer to the new July 15th deadline and the end of the filing season in October 2020.

Because of the COVID-19 pandemic, ETAAC has adjusted its predictive methodology for estimating the overall e-file rate and is using a normalized date of March 6, 2020

---

[122] Pub. L.105–206, 112 Stat. 685, enacted July 22, 1998

[123] Pursuant to its definition of "e-File Rate" in the IRS Strategic Plan 2009-2013 (Pub. 3744, 4-2009), the IRS reported that it would "measure the percentage of all major tax returns filed electronically by individuals, businesses and tax-exempt entities" and that "'Major' tax returns are those in which filers account for income, expenses and/or tax liabilities." IRS has not redefined the term major returns in either of its two subsequent Strategic Plans, i.e., for 2014-2017 or for 2018–2022.

[124] See ETAAC Annual Report to Congress, June 2011, p. 2, Footnote 1.

(and its analog for early March 2019). This date precedes the IRS's announcement of a change in the filing deadline from April 15 to July 15, 2020. Additionally, most stay-at-home orders were issued after this date, which will also affect filing season behavior.[125]

Although predicting the overall e-file rate for individual returns is a very small component of the challenges facing our country, ETAAC believes the ability for the IRS to continue to grow electronic filing remains a good indicator of the stability and capacity of our electronic tax filing system.

IRS has exceeded the 80% electronic filing goal for major returns

The IRS undertook a collaborative public/private partnership with states and the private sector to achieve its 80% electronic filing goal, which was accomplished in 2017. This was a momentous achievement not just for this partnership, but also for the American taxpayer because of the increased convenience and speed of refund delivery associated with electronic filing and direct deposit. Electronic filing rates have steadily increased since 2017.

Table 1: 2017-2020 Electronic Filing Rate for Major Returns

	2017 (IRS Actual)	**2018 (IRS Actual)**	**2019 (IRS estimated)[126]**	**2020 (IRS projected)**
Electronic Filing Rate	80.1%	81.0%	82.2%	83.3%

Source: IRS Publication 6186 (2018 and 2019 Updates). Also see Appendix E.

Overall e-file rates continue to grow, but more slowly

As shown in Table 2 below, the IRS estimates that individual returns have the highest e-file rate and consistently represent over 75% of major returns filed in total. The relatively low growth rate of individual e-file can be expected as individual return e-file matures.

E-file rates continue to increase for other major return types. The Taxpayer First Act, enacted July 1, 2019 implemented an e-file mandate for certain tax returns for exempt organizations. As a result, the overall e-file rate for these returns is expected to grow. It continues to be worth noting, that the employment tax return segment[127] continues to increase, albeit the overall rate of e-file for employment returns remains relatively low. The extension of 2020 due dates for Form 941 may impact electronic filing rates for these returns in the 2020 filing season.

[125] Future analyses of e-file rates will need to account for the inclusion of "simple returns" that were filed in 2020 solely to obtain Economic Impact Payments.

[126] See IRS Publication 6186 (2019 Update), pps. (1) – (3) for the IRS's explanation of its estimate and projection methodologies.

[127] As used in this report, "Form 94X" refers generally to the major employment returns, e.g., Form 940 Employer's Annual Federal Unemployment (FUTA) Tax Return, Form 941 Employer's Quarterly Federal Tax Return, etc.

Table 2: 2020 Projected Electronic Filing Rates

	2019 IRS Estimated			2020 IRS Projected			
	Total	**E-filed**	**E-file Rate**	**Total**	**E-filed**	**E-file Rate**	**Year-over-Year Change**
Individual (Forms 1040, 1040-A, and 1040-EZ)	153,631,200	137,182,700	89.3%	155,100,700	139,840,200	90.2%	.9%
Employment (Form 94X Series)	31,445,700	14,713,400	46.8%	31,718,600	15,551,800	49.1%	2.30%
Corp Income Tax (1120,1120-A,1120-S), etc.	7,425,500	6,034,900	81.3%	7,558,800	6,213,000	82.2%	0.90%
Partnership (Forms 1065/1065-B)	4,319,000	3,831,700	88.8%	4,414,300	3,974,900	90.1%	1.30%
Fiduciary (Form 1041)	3,117,700	2,710,300	87.0%	3,105,900	2,744,000	88.4%	1.40%
Exempt Orgs (Forms 990, 990-EZ, etc.)	1,712,300	1,199,300	70.1%	1,752,000	1,313,700	75.0%	4.90%
Totals	201,651,400	165,672,300	**82.2%**	203,650,300	169,637,600	**83.3%**	1.10%

Source: See Table 2, IRS Publication 6186 (2019 Update)

The 2020 electronic filing rate for individual returns should hit approximately 90%

As of April 10, 2020, the e-file rate for individual returns through the initial part of the 2020 Filing Season was about flat compared to the prior year comparable period.[128]

As in the past, ETAAC has a methodology to estimate the current year individual return e-file rate based on season-to-date filing information adjusted for changes in historical e-file patterns between May and October (See Appendix E). ETAAC has previously explained how that approach has been adjusted given the unique circumstances of this filing season.

Based on its methodology, ETAAC estimates that individual returns should achieve an e-file rate of over 89% for the 2020 filing season, which is consistent with the IRS's 2020 projection in Publication 6186.

Nevertheless, gaps remain in e-file capabilities and measures

ETAAC continues to observe that (i) some return types cannot be e-filed or are not included in the IRS's definition of major returns for purposes of measuring its

[128] See https://www.irs.gov/newsroom/filing-season-statistics-for-week-ending-april-10-2020.

achievement of the 80% rate, and (ii) employment return e-file remains too low – albeit it is growing more rapidly in recent years.

Some returns with sizeable volumes have not be electronically filed

Certain return types are not e e-fileable and must be remitted on paper. One such form is the Amended U.S. Individual Income Tax Return (Form 1040X), of which approximately 3.4 million were filed in 2019.

ETAAC is pleased to acknowledge that the IRS has been working hard to enable the electronic filing of Form 1040X and is projecting implementation of this capability in the second half of 2020.

Some returns with sizeable volumes are not being tracked as part of the 80% goal

As ETAAC noted last year, there are other returns with sizeable or increasing high volumes that are not included in the IRS's definition of major returns. For example, the IRS estimates that the Form 4868 Application for Automatic Extension of Time To File U.S. Income Tax Return will account for over 16 million filings in 2020. If Form 4868 were included in the definition of major returns, ETAAC estimates the overall e-file rate would decrease. Similarly, if Form 1040X returns were included in the definition of "major returns," the IRS's overall e-file rate would also decrease.

Employment return e-file rates remain relatively low

Although its e-file rate has increased year-over-year, employment return e-file rates continue to be approximately one-half of the e-file rate of most other major returns. ETAAC has commented on this area for several years, most recently in our 2018 Annual Report to Congress.

The good news is that the gap is closing at a faster pace. For example, the IRS estimated the e-file rate for employment returns in 2014 to be about 32%. For 2019, the IRS estimated that e-file rate to be almost 47%. A 15% increase over five years is promising. However, the ETAAC encourages the IRS to continue to look for opportunities to increase the e-file rate in this area, e.g., if the IRS's evolving e-signature initiatives would make it easier for employment return filers to register and participate in electronic filing.

Electronic deposits and payments

Another area of focus for electronic tax administration beyond electronic filing is electronic deposits and payments. More regular tracking and reporting of information in this area would supplement the current regular reporting of direct deposit refunds and provide insights to the IRS, states and industry.[129]

IRS Tax Preparation Programs for Lower Income, Elderly and Underserved Taxpayers

Program Overviews

The IRS has two primary programs providing free tax preparation to lower income, the elderly, the underserved and other targeted taxpayer populations – IRS Volunteer

[129] See https://www.irs.gov/newsroom/filing-season-statistics-for-week-ending-may-1-2020.

Programs and the IRS Free File Program. Depending on the program, a variety of factors may affect eligible taxpayer usage including consumer preference and lack of awareness. Other factors for in-person preparation programs could include site capacity, IRS restrictions on the types of returns that can be prepared by volunteer preparers, physical location and hours of operations.

IRS Volunteer Programs (VITA/TCE[130]) – "Assisted Preparation"

- Services Offered. Tax preparation services for specified forms and tax situations are provided by certified volunteers, typically at sites managed by non-profit, religious or educational institutions. Services are normally provided in-person, but some VITAs offer other preparation models typically referred to as drop-off of Virtual VITA.
- IRS Program Management. Program managed by IRS Stakeholder Partnerships, Education & Communication (SPEC), which is in the IRS Wage & Investment Division. There are approximately 300 SPEC employees across country.
- Appropriations and Program Marketing. Congress currently provides dedicated funding of about $25 million for VITA and $11 Million for TCE for use in program matching funds, which would include marketing efforts by Volunteer Tax Program providers. The IRS also promotes Volunteer Tax Programs on irs.gov and in connection with communications campaigns managed by IRS Communications & Liaison.
- Historical Participation Rates. In recent years, VITA/TCE sites have prepared about 3 million of the approximately 90 million individual tax returns prepared by third parties (preparers) for taxpayers, which is about 3.3% of the "assisted" preparation segment.

IRS Free File Program – "Do-it-yourself Preparation" (DIY)

- Services Offered. The Free File Program is a partnership between the IRS and the Free File Alliance, which is a group of ten private-sector tax software companies that have agreed to provide free DIY online tax preparation and electronic filing services to taxpayers.[131] IRS Free File offers two types of preparation models: a full featured interview-based software option subject to certain income and eligibility requirements and, alternatively, a forms-based Free File Fillable Forms option available to all taxpayers regardless of income.[132]
- IRS Program Management. Program managed by a small team within IRS Wage & Investment Division.
- Appropriations and Program Marketing. Congress does not provide any dedicated appropriations for the Free File Program. The IRS does not currently have any budget dedicated to Free File marketing or promotion. However, the

[130] VITA stands for the Volunteer Income Tax Assistance Program and TCE stands for Tax Counseling for the Elderly Program.

[131] https://www.irs.gov/e-file-providers/about-the-free-file-alliance

[132] https://www.irs.gov/filing/free-file-do-your-federal-taxes-for-free

IRS does promote Free File on irs.gov and in connection with communications campaigns managed by IRS Communications & Liaison.

- Historical Participation Rates. In recent years, Free File offerings have been used to prepare about 2.8 million returns of the approximately 65 million individual tax returns self-prepared by taxpayers, which is about 4.3% of the “DIY” preparation segment.

2020 Filing Season Program Observations

IRS Volunteer Programs (VITA/TCE)

The IRS Volunteer Programs provide an important service to taxpayers, and ETAAC supports continued Congressional appropriations for them.

The COVID-19 pandemic has created a challenging 2020 for the IRS Volunteer Programs. Essentially all VITA and TCE sites have terminated their traditional in-person services to protect the health of taxpayers and staff. Additionally, the capacity of some sites have been impacted by reduced volunteer availability because many volunteers are older Americans and, hence, more vulnerable to the virus.

In response, many program sites have worked aggressively (and creatively) to develop and execute back-up plans that includes drop-off and virtual tax preparation services. Programs have been very thoughtful in executing these service models to ensure the health and safety of taxpayer and staff, as well as to protect taxpayer information. The IRS has also worked closely with these programs to implement secure modes of completing identity verification, submitting documents and obtaining taxpayer signatures.

One key learning from this experience is that technology is instrumental in enabling volunteer programs to deliver services that meet social distancing guidelines. Some examples include using: Zoom to conduct client interviews, JotForm to enroll clients for services and DocuSign to obtain client signatures. VITA programs have also collaborated with their partners to develop services, e.g., VITA is working with a non-profit called Code for America to design and implement a totally virtual model for serving clients. VITA programs are also more promoting “facilitated self-assessment” (DIY) tax preparation support.

The continuation of the COVID-19 pandemic through the rest of 2020 and into 2021 will continue to impact VITA program costs and how they provide their services.

But, the demands being driven by COVID-19 will not end with some vaccine. As in so many other areas, COVID-19 is forcing a scrutiny of existing service delivery models and exposing opportunities to better deliver services. In the case of VITA, for example, that includes identifying new ways to reach and serve low income and under-served communities. IRS SPEC should actively support and enable these new game-changing service models.

IRS Free File Program

The IRS Free File Program provides an important service to taxpayers, and ETAAC supports the IRS's continued investment in this partnership.

As demonstrated this filing season, the program's DIY offerings are an important complement to the IRS Volunteer Programs' assisted preparation offerings.[133] As of mid-April 2020, the IRS reported a record increase in Free File volumes -- 2.9 million tax returns year-to-date, which is a 28% increase compared to the 2.3 million received during the same time in 2019 and exceeds the number of returns received during all of 2019.[134]

ETAAC supports the Commissioner's continued actions to improve the Free File Program, which could include creating an overall program strategy, increasing taxpayer awareness, measuring user satisfaction and effecting ongoing IRS monitoring and oversight, and maintaining an adequate number of qualified Free File participating companies.[135] The 2020 filing season presents an opportunity to assess the impact of the IRS's recent amendments to the program and consider other opportunities to improve it.

Finally, the Free File partnership also enabled the IRS to rapidly develop and deploy an industry-provided Non-Filer Tool (described above) to facilitate the direct deposit of Economic Impact Payments under the CARES Act, instead of forcing taxpayers to wait weeks for a mailed check.

[133] In ETAAC members' experience, taxpayers tend to self-identify in one of two preference categories: (i) they prefer to have someone else prepare their return, or (ii) they prefer to prepare their own returns. A variety of factors influence these preferences. For example, those taxpayers who prepare their returns tend to have more confidence in their own ability to prepare their return and want control over the preparation process. On the other hand, those preferring to have someone else prepare their return may lack the understanding or confidence of preparing their own return (even simple returns), lack the time to prepare their return or view return preparation as an inconvenience (even if they have the time). Although there is some movement between these two preference categories, it seems to be relatively limited.

[134] IRS News Release IR-2020-74 (April 16, 2020) (https://www.irs.gov/newsroom/irs-free-file-use-soars-taxpayers-still-have-time-to-do-their-taxes-for-free).

[135] Numerous stakeholders have made recommendations to improve the Program, including TIGTA, the Taxpayer Advocate and the IRS Advisory Council (IRSAC).

PROGRESS ON ETAAC 2019 AND 2018 RECOMMENDATIONS

ETAAC's recommendations are provided for consideration by the IRS, which will ultimately determine whether and how to implement them based on its assessment of benefit/cost and competing priorities.

Progress on ETAAC 2019 Recommendations

Congressional Action

ETAAC is pleased to recognize the progress on its 2019 Recommendation #2 to enact an IDTTRF exception to IRC Section 6103. Specifically, this recommendation was addressed by Section 2003 of the Taxpayer First Act.

As yet, Congress has not acted on ETAAC's 2019 Recommendation #7 to grant the IRS the authority to establish and enforce security standards. ETAAC continues to believe the absence of this authority presents a risk to taxpayers and our tax system, and is making a comparable recommendation in its 2020 Report (See Recommendation #4 in this Report).

IRS Action

The IRS responded to ETAAC's 2019 recommendations in September and October 2019 and generally agreed with them with one exception. Specifically, with respect to Recommendation #7 to grant the IRS the authority to establish and enforce security standards, the IRS disagreed with ETAAC stating that "The IRS currently has neither the funding nor staffing at a level possible to support such a program, especially if it is to be implemented similar to the assessment program implemented by the Office of Safeguards for reviewing how the states implement and maintain appropriate information security standards and practices."

ETAAC has two thoughts. First, ETAAC agrees that the IRS would need the funding and staffing to undertake this activity. Second, ETAAC has not proposed that the IRS should implement a security program "similar to the assessment program implemented by the Office of Safeguards for reviewing how the states implement and maintain appropriate information security standards and practices." In fact, ETAAC believes this approach could be counter-productive, especially concerning tax professionals.

However, ETAAC continues to believe the absence of this authority (and associated funding) presents a risk to taxpayers and our tax system. For that reason, ETAAC is making comparable recommendations in its 2020 Report. (See ETAAC 2020 Report's Recommendation #4 concerning IRS authority and Recommendation #7 concerning the conduct of a study to inform actions in this area).

With respect to the remainder of its 2019 recommendations, ETAAC believes that the IRS has or is taking appropriate action to date:

- Funding the ISAC (Recommendation #1)
- Implementing the IDTTRF exception to IRC Section 6103 in to the ISAC (Recommendation #2)
- Increasing the engagement of ISAC members (Recommendation #3)

- Integrating the Payroll Community more fully into the Security Summit (Recommendation #4)
- Piloting a Financial Services Company (FSC) Collaboration Space in the ISAC (Recommendation #5)
- Developing and expanding channels for identity proofing (Recommendation #8)
- Collaborating with Security Summit members to identify and pilot emerging approaches for identity verification (Recommendation #9)
- Engaging with the Security Summit to improve the Taxpayer Protection Program's taxpayer experience (Recommendation #10)

ETAAC is not aware of any progress on Recommendation #6 to "assess the state of information security practices in the tax professional community."[136]

Continuing Attention on ETAAC's 2018 Recommendation #10

Over the past three years, ETAAC has expressed a continuing concern about the lack of a single IRS owner or coordinator for security standards and practices across the tax industry.

In 2018, ETAAC Recommendation #10 proposed that "The IRS should identify and empower one organization inside the agency with overall responsibility for setting security requirements for tax professionals and coordinating the implementation of such requirements across IRS stakeholders." (The IRS did not provide a response to this recommendation.)

Our 2019 Report restated this concern:

> "As noted in our 2018 Report, ETAAC believes that the IRS needs a "single owner" and that tax professional information security should not be based on whether someone is a CPA, EA, Attorney or unenrolled preparer. They are all tax professionals holding taxpayer information that is at risk. We have concerns about the efficiency of the IRS managing tax professional security by distributing this responsibility within its existing organizational structure that manage the various categories of tax professionals, e.g., preparers, practitioners, VITA volunteers and EROs.
>
> ETAAC's characterization of a "single owner" refers to the designation of a specific IRS organization (existing or new) which would be responsible for working with current IRS functions responsible for the tax professional community to facilitate the development and execution of a cohesive, coordinated tax professional security strategy."

This issue remains a continuing concern not just for ETAAC, but for GAO.[137]

[136] ETAAC requested an update on any progress or action on this recommendation in early February.

[137] See Recommendation #1 (and IRS response) in GAO Third Party Cybersecurity Report.

Appendix A

About ETAAC

Initial Focus

The Electronic Tax Administration Advisory Committee (ETAAC) was formed and authorized under the Internal Revenue Service Restructuring and Reform Act of 1998 (RRA 98). The historical charter of ETAAC was to provide input to the Internal Revenue Service on electronic tax administration.

ETAAC's responsibilities involve researching, analyzing, and making recommendations on a wide range of electronic tax administration issues. Additionally, pursuant to RRA 98, ETAAC reports annually to Congress concerning:

- The IRS's progress on reaching its goal to electronically receive 80% of tax and information returns;
- Legislative changes assisting the IRS in meeting the 80% goal;
- Status of the IRS strategic plan for electronic tax administration; and
- Effects of e-filing tax and information returns on small businesses and the self-employed.

Expanded Focus

In March of 2015, the IRS assembled a coalition of IRS, tax industry and state revenue agency leaders to undertake a major initiative to combat IDTTRF by creating what has become the IRS Security Summit.

In 2016, the IRS amended the ETAAC charter to expand ETAAC's focus to address the serious problem of IDTTRF, which was threatening to erode the integrity of the tax system. In 2019, Congress statutorily confirmed this expansion of responsibilities in Section 2002 of the Taxpayer First Act. As a result, ETAAC will continue to provide strategic and operational recommendations on combating IDTTRF and improving information security.

Coincident with these changes, ETAAC has expanded its authorized size to broaden the experience of its members and add new stakeholder perspectives from the government, commercial, non-profit and consumer sectors. ETAAC members come from state departments of revenue, large tax preparation companies, low-income and consumer advocacy groups, solo tax practitioners, tax and accounting software companies and the financial services industry. (See Appendix B for ETAAC member biographies.)

How ETAAC does its work

In conducting its assessments and formulating its recommendations, ETAAC relies on a variety of information sources. Most importantly, ETAAC participates in numerous discussions with IRS representatives and Security Summit participants. Many of the ideas that ETAAC has incorporated into its recommendations arose in these discussions and are already being considered or acted upon by the Security Summit Work Groups.

ETAAC also reviews reports from a variety of sources, including other advisory boards, the National Taxpayer Advocate, the Government Accountability Office (GAO), and the Treasury Inspector General for Tax Administration (TIGTA). The Committee is most grateful for their observations. On occasion, ETAAC may also seek background insights from policy leaders, industry and state revenue agencies as well as other experts.

Then, ETAAC members use this information and these insights to develop the ETAAC's annual report in a highly collaborative and rigorous deliberation and drafting process. Any recommendations and opinions expressed in this Report are solely those of ETAAC.

Public comments on this Report may be sent to etaac@irs.gov.

Appendix B

ETAAC Member Biographies

Luanne Brown - Brown has served as the Director of Payroll Services for Grand Valley State University for the last 13 years. For more than 20 years she has worked in varied industries including sports management, advertising, manufacturing, and higher education. In her current role at the University there has been a major emphasis on data security. She has participated on a Senior Management Cyber Security Team and helped develop new security procedures and policies in the Payroll/Finance area along with communicating to employees on how to protect their personal data from identity theft and steps to take if their information has been compromised. Brown currently serves as a Director on the American Payroll Association Board of Directors. Brown holds a master's degree in Public Administration with an emphasis on Public Management from Grand Valley State University.

Latryna Carlton - Carlton is President of Committed Citizens of Waverly (CCOW Inc.) in Waverly, Fla., a community-based organization dedicated to self-help and volunteering. Carlton is a Volunteer Income Tax Assistance (VITA) site coordinator and trainer.

Daniel Eubanks - Eubanks is Senior Manager for Federal Government Relations at Intuit. He serves as an Industry co-lead on the Security Summit Authentication Working Group. Eubanks previously served on the Board of Directors for CERCA (the Council for Electronic Revenue Communication Advancement), as well as the Senior Executive Board of the Identity Theft Tax Refund Fraud Information Sharing and Analysis Center.

Larry Gray - Gray is a certified public accountant with his own firm, Alfermann Gray & Co. Gray serves on the Security Summit Tax Professionals Working Group. He is an instructor for the National Association of Tax Professionals (NATP) and speaks regularly at the IRS Nationwide Tax Forums.

Jenine Hallings - Hallings is a Compliance Risk Manager for Paychex. Her team is responsible for research, analysis and communication of legislative and regulatory changes impacting the company and its clients and partners, and manages Paychex' relationships with various federal and state tax agencies on behalf of clients. Hallings represents Paychex in key industry consortiums to ensure the company is abreast of regulatory trends and developments. Hallings has been at Paychex for over 20 years, and has extensive experience on a broad range of payroll tax and privacy matters. Hallings holds an MBA from the Rochester Institute of Technology.

Michael Jackman - Jackman is a Senior Cybersecurity Analyst for Maximus Federal, and has extensive experience in taxation, tax administration and related information systems. He currently operates a small tax practice and serves as the coordinator for two Volunteer Income Tax Assistance (VITA) sites. Over a 22-year tenure as an IRS employee he held several compliance and information technology positions, culminating in serving in the IRS National Office as the Chief of Systems Development for the original Electronic Filing System. As a consultant, he provided

expertise to the IRS in the development of numerous IRS information systems including Modernized E-File, and the Customer Account Data Engine (CADE). In addition, he owned and operated several Jackson Hewitt Tax Service franchises in Maryland, after which he founded Patriot's Choice Tax Service in Gettysburg. Jackman is an Enrolled Agent and holds an MS in Taxation from the Deming School of Business at William Howard Taft University.

John Kreger - Kreger is Director of Product Management at Sovos, where he leads the team responsible for Sovos' 1099, ACA, and Insurance Premium Tax reporting solutions. He has experience as a software developer, solution engineer and information systems manager.

Suzanne Kruger – Kruger currently serves as the Security Specialist for the Montana Department of Revenue and on several committees for the Montana Information Security Advisory Council (MT-ISAC). She has more than 26 years of experience working with state government, businesses, non-profits and individuals in the accounting, tax preparation and banking fields. She holds degrees in Network Security and Network Administration and the following certifications; ISC2 - Certified Information Systems Security Professional (CISSP) and ISC2 - Certified Authorization Professional (CAP).

Laura Macca - Macca is National Director of Business Transformation at EisnerAmper. Previously, Macca led tax process, policy, digital transformation and risk management initiatives as Chief of Staff at Bridgewater Associates LP. She is a certified public accountant and member of the American Institute of CPAs (AICPA).

Julie Magee - Magee is Director of Tax Regulatory Affairs at Credit Karma Tax, Inc. She is a founding participant in the Security Summit and the Identity Theft Tax Refund Fraud Information Sharing and Analysis Center. She serves on several Summit working groups. Magee was previously Commissioner of the Alabama Department of Revenue and held leadership roles at the Federation of Tax Administrators, the Multistate Tax Commission, and the Southeastern Association of Tax Administrators.

Ada Navarro - Navarro is Lead Examiner for the Fraud Unit of the Connecticut Department of Revenue Services, handling both civil and criminal tax fraud cases. Navarro is co-project manager for Connecticut's paid preparer legislation committee. Her memberships and associations include the Identity Theft Tax Refund Fraud Information Sharing Analysis Center, the Federation of Tax Administrators, the Suspicious Filer Exchange Program, the International Association of Financial Crimes Investigators and the National White Collar Crime Center.

Kathy Pickering, EA - Pickering is the Chief Tax Officer of H&R Block. With over 20 years of experience in tax administration, Kathy is responsible for the strategic direction and management of a team of the nation's top tax experts. As head of The Tax Institute, Pickering oversees a group of 23 credentialed tax experts, with deep knowledge of the industry and regular, direct interaction with tax professionals and taxpayers. This team provides four key functions: 1) providing expert research and analysis to frontline tax professionals and taxpayers, 2) tax law and policy analysis, 3) leading the identification, communication, and integration of tax changes across

H&R Block's operations, and 4) coordination and communication among the IRS, state and local agencies on issues affecting the tax industry. In her role as H&R Block's vice president of regulatory affairs, she leads the relationship-management strategy with the IRS and state taxing agencies. Pickering is currently focusing on the IRS Security Summit, which brings together representatives from the IRS, state tax agencies, and private industry to work on collaborative solutions to combat stolen identity refund fraud schemes.

Phillip L. Poirier, Jr. - Poirier is a volunteer tax preparer in the IRS Volunteer Income Tax Assistance (VITA) program and is active in the Taxpayer Opportunity Network, which is managed by Prosperity Now and supports VITA programs at the national level. He is also a Senior Fellow with the Center for Social Development at Washington University in St. Louis. His consulting work with academia, non-profits and foundations focuses on investigating ways to better leverage the U.S. tax system to improve individual and family financial well-being in personal finance, credit, asset building and savings, as well on improving information security. His previous employment included working as an in-house lawyer and executive in the tax software industry with Intuit Inc. and practicing law in a private firm. Poirier served in the U.S. Navy and Naval Reserve for nearly three decades, retiring as a Captain. He holds a J.D. from the University of San Diego School of Law, and a bachelor's degree in international affairs from the United States Naval Academy.

Lynnette T. Riley - Riley was appointed by Governor Brian P. Kemp to serve as Georgia's first woman to hold the office of State Treasurer in May 2019. Previously, Governor Nathan Deal appointed Riley to serve as State Revenue Commissioner in 2015, a role she performed for over 4 years. Elected to the Georgia General Assembly in 2010, State Representative Riley was the Fulton County House Delegation Chair during the 2013-2014 Legislative Session, and she served as one of Governor Nathan Deal's Floor Leaders in 2014. Treasurer Riley served in local government as the District 3 Fulton County Commissioner from July 2004 to December 2010. Riley currently serves on the Executive Committee of the National Association of State Auditors, Comptrollers and Treasurers (NASACT) and is Vice-Chair of the Legislative Committee of the National Association of State Treasurers (NAST). As Georgia's State Treasurer, Riley is the administrative officer and board member of the State Depository Board, the Georgia Higher Education Savings Plan Board and the Georgia ABLE Program Corporation board. Riley served on the IDTTRF-ISAC Senior Executive Board from 2017 to 2019.

Cynthia Rowley - Rowley is Assistant Commissioner at the Minnesota Department of Revenue, responsible for the Department's Individual Income and Withholding Division, Property Tax Division, and Tax Operations Division and Special Tax Division. Rowley was previously Director of Property Tax and Director of the Tax Operations Division. She is a member of the Federation of Tax Administrators.

Gene Salo - Salo has over 25 years of experience in the tax industry, initially in tax preparation and later in tax software development. Recently, Salo has turned his focus to identity theft and tax refund fraud. He is active with the IRS, state tax agencies and tax industry members in the Security Summit, where he is a co-lead

for the Tax Professional Working Group. Salo also serves as the Vice Chairman of the Board of Directors of CERCA, an association of tax industry firms that supports electronic filing. Salo earned his MBA from the University of Michigan and has a dual BA in Accounting and Finance from Oakland University. He is a veteran of the US Air Force.

John Sapp - Sapp has served a key role at Drake Software for over 20 years, with roles ranging from Chief Financial Officer to Vice President of Drake's Sales and Marketing divisions. Today he serves as the Vice President of Strategic Development, where his role is to help shape the future and growth of one of the largest professional tax software companies in the nation. As a CPA, he has considerable experience working in public accounting in technological and private industries. He holds a bachelor's degree in Accounting from Oral Roberts University.

Joseph Sica - Sica, Chief Public Policy Officer for Green Dot/Tax Products Group, has been affiliated with tax time financial products and combating fraud in the tax system for the last 28 years. In the earliest days of e-filing, Sica worked with the IRS to develop and pilot refund loans as an incentive for people to file electronically. Prior to IRS having increased fraud detection capabilities, he started the Fraud Service Bureau in 1994 in which banks in the tax loan industry electronically exchanged data to identify fraud and shared results with the IRS. Years ago, Sica changed his primary focus in the tax industry from technology to related policy affairs and assisted in coordination of dialog between the industry and the IRS. As such, he is a co-founding board member and past chair of the Council for Electronic Revenue Communications Advancement (CERCA). Sica is also a co-founder member and past vice-chair of the American Coalition for Taxpayer Rights (ACTR), a tax industry policy group seeking to preserve taxpayer choices. Recently, he has worked with industry, state revenue departments and the IRS in connection with establishing the IRS Security Summit taking co-lead roles in the Information Sharing and the Financial Services work groups. Sica completed Executive Development work at The Wharton School in 1996.

Mark Steber - Steber, Chief Tax Officer with Jackson Hewitt Tax Service, is responsible for several key initiatives to support overall tax service delivery and quality assurance. Steber serves as a Jackson Hewitt liaison with the Internal Revenue Service, States, other government authorities, Walmart, other retail entities, and banking partners. With over 30 years of tax experience, Steber is widely referenced as an expert on consumer income tax issues and especially electronic tax and data protection issues. Steber has been an active participant in the IRS Security Summit Initiative since the founding of the effort in early 2015. He has been involved with all the work groups including the Information Sharing Group, Authentication Work Group and Strategic Threat Assessment and Response (STARS) group and subsequent new groups including the Tax Pro Subgroup of the Security Summit. Steber is active with various industry groups, including ACTR and CERCA, and has worked directly with leadership members in many instances. In prior years, he served on the IRS Electronic Tax Administration Advisory Committee and was Chairman in 2012. Prior to joining Jackson Hewitt, he was a tax partner with Ernst and Young LLP.

Matthew Vickers - Vickers is General Manager of Product for U.S.-based Xero Inc. and its publicly listed New Zealand-based parent company Xero Limited. Xero offers online accounting and tax-filing software to small businesses. Vickers participates in multiple US and global industry forums, particularly in relation to standardized business documents. Vickers also serves on the Board of Directors for the Data Coalition, a DC-based trade association that advocates for responsible policies to make government data high-quality, accessible, and useable.

Appendix C

IRS Modernization Business Plan FY2020 Scheduled Deliverables

MODERNIZATION PILLAR	CAPABILITIES SCHEDULED FOR DELIVERY IN FY2020
Taxpayer Experience: Deliver a service experience comparable to private industry	**WebApps** • Taxpayer Payment API with Fiscal Service – View Payments Release 1 • Modernize Online Installment Agreements – View Status and Eligibility Release 1 **Live Assistance – Callback** • Customer Callback 2020 – Additional 4 taxpayer applications • Expanded toll-free capacity
Core Taxpayer Services & Enforcement: Streamline and integrate IT programs that enable top-quality service	**CADE 2 TS2** • Measurable progress toward converting code with a target of 31% focusing on developing multiple Scenario variations of the Address Change transaction • Measurable progress toward converting code with a target of 35% and with a focus on Scenarios for input transactions when an account is not present in the master file • Measurable progress toward converting code with a target of 38% and with a focus on scenario functionality yet to be planned iteratively • Measurable progress toward converting code of 43%, specific focus on scenario functionality yet to be planned iteratively **Enterprise Case Management (ECM)** • Procure ECM solution • Deliver initial case management capabilities
Modernized IRS Operations: Retire and decommission legacy systems in place of more sustainable infrastructure	**Robotic Process Automation (RPA)** • SB/SE Monitoring Offer in Compromise (MOIC) • IT Help Desk Self-Service (Natural language processing) • TE/GE Referrals Batch Process Identification **Application Programming Interface (API) Implementation** • Leverage security efforts with 3rd parties to develop API(s) **Cloud Execution** • Procure and deliver ECM Release 1 Cloud platform on Treasury Cloud • Deploy Cyber CDM Phase 2 on Treasury Cloud **Next Generation Infrastructure** • DevOps: CI/CD Onboard additional projects • DevOps/Standard Stack: Deploy 3 to 5 standard stack components via automation • DevOps/Standard Stack: Develop and deploy additional standard stack components • Converting Legacy Code / Reducing the Application Footprint: Strategy on Legacy Code Conversion
Cybersecurity & Data Protection: Continue to protect taxpayer data and address emerging threats	**Vulnerability & Threat Management** • Complete IT Asset Management Use Case • Pilot Data at Rest Encryption (DARE) • Enhanced Security Testing (EST) and Process Automation • Expand DARE implementation • Enhanced Cyber User Behavior and Fraud Analytics IOC • Next Generation ESAT (Limited IOC) • Enhanced EST and Process Automation IOC **Identity & Access Management** • CDM Phase 1 FOC • CDM Phase 2 IOC • Convert 12 facilities for physical access compliance **Security Operations & Management** • Malware Email Sandboxing FOC • Endpoint Detection Response IOC • Continue network access restriction in Enforcement Mode implementation • IRS Cloud Access Security Broker (CASB) FOC • Malware Web Sandboxing FOC • Cyber Hyper Converged Infrastructure FOC for Real-Time Correlation Analysis • Endpoint Detection Response FOC • Begin network segmentation for High Value Assets (HVA)

Appendix D

ETAAC Observations to IRS TFA Program Office

……..

MEMORANDUM

From: Phillip Poirier, ETAAC Chair

To: Lisa Beard, IRS Taxpayer First Act Office

Copy: John Lipold and William Parman, IRS NPL

ETAAC Members

Date: April 1, 2020

Subj: Taxpayer First Act (TFA) Section 1302

TAXPAYER FIRST ACT

Thank you for meeting with ETAAC during our January 2020 meeting.

One area of discussion was TFA Section 1302, which requires the IRS to submit a comprehensive written plan to Congress to redesign the organization of the Internal Revenue Service to, among other things:

- *Streamline the structure of the agency including minimizing the duplication of services and responsibilities within the agency,* and
- *Best position the Internal Revenue Service to combat cybersecurity and other threats to the Internal Revenue Service.*

We understand that your submission deadline to Congress has been accelerated to July 2020. Because our Annual Report to Congress does not issue until late June 2020, ETAAC is providing this memorandum now so that our views can be timely considered.

ETAAC has three high-level observations relevant to the above TFA provisions (background and supporting details follow):

1. Identifying a single IRS organization to manage or coordinate IRS requirements, policy and oversight of tax preparer security.
2. Designating an IRS organization responsible for evaluating and responding to threats to disrupt our public/private tax system, which goes beyond cybersecurity and may actually go beyond what we currently consider to be the "tax ecosystem."[138]

[138] That is, there may be inputs to our income and payroll tax systems that could be disrupted, which would affect downstream operations and, ultimately, submissions to IRS. Similarly, such disruptions may not involve data breaches. For example, MeF could be a very operational secure system, but an adversary might chose to attack private sector inputs to MeF. The distributed nature of the private sector income and payroll tax system is a strength, but its risks and vulnerabilities should be understood and planned for.

3. Anticipating and addressing the impacts of any IRS redesign on the management and oversight of the IRS Security Summit, including the ISAC.

Thank you for the opportunity to submit comments on this important topic.

BACKGROUND

The security and operation of our public/private tax system present risks

Every year, the federal tax system generates about $3.5 trillion dollars in collections that fund about 95% of government operations and deliver approximately $350 billion in tax refunds.

That federal tax system is a highly integrated public/private system that includes not just the IRS but also non-governmental third parties, e.g., tax preparation technology sector, tax and payroll professionals, financial institutions, and others. As a result, the risks associated with the security and operation of the overall tax system extend well beyond the IRS's boundaries.

ETAAC sees two distinct albeit related risks (and potential gaps) in this broader area:

- ***Cybersecurity Risks*** – efforts to access tax information without authorization for the purpose of financial gain such as stolen identity refund fraud (most commonly cybercriminals)
- ***Disruption Of Service Risks*** – efforts to disrupt the operation of our government or economy by interrupting the flow of tax revenue to our government or tax refunds into our economy (most likely nation states or their proxies, albeit ransomware cybercriminals might try to leverage disruption activities)

No single IRS function has overall responsibility to coordinate the security of the private sector tax system

The private sector component of our tax system has several participant segments that have varying levels of cybersecurity sophistication – anywhere from large nationwide tax software and branded retail preparation companies with dedicated and experienced cybersecurity staffs to smaller and less sophisticated local solo and small practice tax preparers.

Currently, IRS Cybersecurity is working with the electronic tax industry (income tax and payroll) to establish and implement heightened security standards based on the NIST cybersecurity framework. That makes perfect sense to ETAAC.

On the other hand, the IRS's current approach to manage or coordinate the security of "tax professionals" is problematic. (For our purposes, tax professionals include tax practitioners, unenrolled tax preparers and volunteer VITA/TCE preparers – and the businesses or organizations through which they provide their services)

ETAAC is not aware of any single IRS organization with the overall responsibility to understand, monitor and coordinate or manage the security risks and vulnerabilities with a focus on private sector operations.

In the tax professional area, for example, GAO reported that multiple IRS functions are involved in monitoring, communicating and/or engaging with tax professionals around security, including:[139]

- Return Preparer Office (RPO)
- IRS Cybersecurity
- W&I Division: Customer Account Services (CAS)
    - Electronic Products and Services (EPSS)
- W&I Division: Customer Assistance, Relationships and Education (CARE)
    - Stakeholder Partnerships, Education & Communication (SPEC)
- Small Business/Self-employed (SB/SE)[140]
- IRS Communications and Liaison
    - Stakeholder Liaison

ETAAC has raised this concern in past reports.[141]

To some extent, this makes sense from an *execution* perspective. However, from a policy and overall management perspective, it creates several problems.

First, it's inefficient and duplicative – IRS functions that do not possess security expertise seem to be leading the development of security policy or guidance. Second, it's difficult to coordinate a clear, consistent message to tax professionals if different functions are driving different messages. Finally, it is confusing to tax professionals when they receive multiple sources of guidance from the IRS. Where do they look for their "final" security guidance – Pub 1345? Pub 4557? NIST Security Guide for Small Businesses? FTC Safeguards Rule?

The same individual could be getting different or duplicative security guidance depending on what hat he or she is wearing, e.g., ERO vs. practitioner vs. unenrolled preparer. It is overwhelming.

ETAAC has raised this issue before. Our 2018 Report to Congress Recommendation #10 provided that "*The IRS should identify and empower one organization inside the agency with overall responsibility for setting security requirements for tax professionals and coordinating the implementation of such requirements across IRS stakeholders*." We did not get a response to our 2018 recommendation. (We made a related observation in our 2019 ETAAC Report to Congress, p. 40)

---

[139] For a good overview of most of these IRS organizations security-related activities, see GAO Report, " TAXPAYER INFORMATION: IRS Needs to Improve Oversight of Third-Party Cybersecurity Practices," May, 2019, pps. 9-11 ("GAO Third-Party Cybersecurity Report").

[140] Pursuant to the Internal Revenue Manual (IRM) Part **4.21.1.19(13) on "**Monitoring Techniques/Security," SB/SE examiners visiting tax professionals acting as Electronic Return Originators should "determine the answers to the following questions:…Is there a security plan? If yes, review the security plan."

[141] See 2018 ETAAC Report to Congress, Recommendation #10. See also related observations in 2019 ETAAC Report to Congress, p. 40.

In 2019, the GAO reviewed third party cybersecurity and made a similar recommendation. GAO recommended that "*The Commissioner of Internal Revenue should develop a governance structure or other form of centralized leadership, such as a steering committee, to coordinate all aspects of IRS's efforts to protect taxpayer information while at third-party providers.*"[142]

The IRS disagreed with GAO and advised that to effectively establish data safeguarding policies and implement strategies enforcing compliance with those policies, a centralized leadership structure requires the statutory authority that clearly communicates the authority of the IRS to do so. Without such authority, the IRS believed that implementing the recommendation would be an inefficient, ineffective, and costly use of resources. GAO disagreed with IRS.

ETAAC agrees it would help if IRS had clearer authority, but does not agree that such authority is required to manage this area in a more coordinated way

ETAAC appreciates that IRS would benefit from having clearer statutory authority in the areas of setting and enforcing security standards. Our 2020 Report to Congress will (again) call for this authority.

However, ETAAC does not agree that IRS cannot act to better coordinate its activities in the absence of such authority. It doesn't make sense to ETAAC that IRS is blocked from creating (at a minimum) a steering committee to coordinate security programs without further statutory authority. It also doesn't make sense to ETAAC that it would be "inefficient, ineffective, and costly" to coordinate security activities focused on a tax professional rather than have five or six IRS groups conducting their tax professional security activities independently.

There should be a clear allocation of responsibility and authority for policy and guidance development based on specific expertise, although such policy or guidance should have input from and could be implemented through multiple channels.

"Disruption of service" risk presents a vulnerability for IRS and our tax system

ETAAC agrees with IRS's focus on cybersecurity risks. However, ETAAC is concerned that cybercriminals are only one threat.

The greater threat to the tax system may be nation state actors or their proxies. For example, the Chinese have been accused of two of the biggest breaches in our nation's history – 21 million people in the 2015 breach of the Office of Personnel Management (OPM)[143] and 148 million people in the 2017 breach of Equifax.[144] How could a foreign adversary use that information?

[142] See GAO Third-Party Cybersecurity Report.

[143] See https://www.nytimes.com/2015/06/05/us/breach-in-a-federal-computer-system-exposes-personnel-data.html

[144] See https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-four-members-china-s-military

In its 9th Annual Cost of Cybercrime Study, Ponemon Institute and Accenture found that cyberattacks are changing in several ways including (emphasis added)[145]:

- Evolving targets: Information theft is the most expensive and fastest rising consequence of cybercrime — but *data is not the only target*. Core systems, such as industrial control systems, are *being hacked in a powerful move to disrupt and destroy*.
- Evolving impact: While data remains a target, theft is not always the outcome. A new wave of *cyberattacks sees data no longer simply being copied but being destroyed — or changed* — which breeds distrust. Attacking data integrity is the next frontier.

*****

Clearly, a disruption of the tax system would create significant challenges for the IRS and nation. (The coronavirus pandemic is just one illustration of a disruption risk.)

Given that, what organization in IRS is looking across the entire public/private landscape to understand how an adversary could disrupt our tax system? In fact, those disruptive attacks might start with activities outside the public/private tax system and not even be associated with a cybersecurity threat vector.

ETAAC believes that an IRS function should have the responsibility to identify, assess, plan for, monitor and manage the tax ecosystem disruption risk on a consistent operational basis, which may include touchpoints with the IRS's enterprise risk management and business continuity planning functions.

IRS leadership is essential to the success of the Security Summit

The IRS's leadership of the Security Summit is critical to its continuing success. Any reduction in effective, focused IRS leadership could cause this unprecedented initiative to wane or fail at a time when the cybercriminals and adversaries are waiting at the gates to steal billions of dollars.

A big part of IRS's successful leadership of the Security Summit is the level of centralized oversight, management and coordination provided by IRS RICS. The Summit Work Groups need this measure of centralized management and coordination to maintain their focus, accountability and cohesion. Any redesign of the IRS should contemplate the oversight and management of the Security Summit, and ensure its viability.

ETAAC OBSERVATIONS

#1: The IRS should identify and empower one organization (or establish a structure like a steering group) inside the agency with overall responsibility for understanding the cybersecurity environment, setting or coordinating security requirements and/or guidance across the tax preparation community (including tax professionals), and coordinating the implementation of such requirements across and through IRS stakeholders.

[145] Ninth Annual Cost of Cybercrime Study, p. 6 (March 2019). See https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf

#2: The IRS should identify and empower one organization (or establish a structure like a steering group) inside the agency with overall responsibility for understanding, assessing and coordinating a response plan to the disruption threats to the entire end-to-end tax system.

#3: As it considers any redesign of its organization, the IRS should carefully consider the impact of any such changes on its leadership and management of the IRS Security Summit and ISAC, and make any necessary adjustments.

Appendix E

ETAAC E-File Analytical Methodology

This Appendix explains ETAAC's methodology for analyzing and projecting annual electronic filling rates for all major returns and for individual tax returns. ETAAC standardized its methodology for e-file estimates and projections to provide a consistent measure of IRS e-file performance, standardize cross-year comparisons and facilitate analysis.

E-file Rates for Major Returns

To determine the e-file rate for all major returns, ETAAC takes two steps.

First, ETAAC utilized the "major" returns, which are used by the IRS as major return categories found in Table 2 of IRS Publication 6186:

Individual Income Tax (Form 1040 series)	Employment (Form 94X series)
Corporation Income Tax (Form 1120 series)	Fiduciary (Form 1041)
Exempt Organizations (Form 990 series)	Partnership (Form 1065 series)

Second, using the IRS' most up-to-date published information from Publication 6186, ETAAC computes an electronic filing rate for each specified return family as well as an overall electronic filing rate for all major return families. These estimates and projections are reflected in Table 2 in the Electronic Tax Administration & Progress Toward 80% E-file Goal section of this Report.

ETAAC-projection for Current Year E-file Rate for Individual Returns

Form 1040 series returns are the largest category of tax returns by volume for IRS e-file given they account for 76% of all major return types.

In its projection for the current year, IRS Publication 6186 primarily relies on historical information as the foundation for its estimates and projections going forward. We, in turn, have used IRS estimates and projections from IRS Publication 6186 as a baseline for ETAAC's projection.

To supplement insights from IRS Publication 6186, ETAAC historically has used a methodology to project the current-year e-file rate for individual returns based on partial filing season data for current year and historical trends. Specifically, the methodology extrapolates and adjusts current filing season year-to-date information into full-year estimates based on historical e-file trends in the May-October period.

Because of the COVID-19 pandemic, ETAAC has adjusted its predictive methodology for estimating the overall E-File rate and is using a normalized date of March 6, 2020 (and its analog for early March 2019). This date precedes the IRS's announcement of a change in the filing deadline from April 15 to July 15, 2020. Additionally, most stay-at-home orders were issued after this date, which will also affect filing season behavior.

Although predicting the overall e-file rate for individual returns is a very small component of the challenges facing our country, we believe the ability for the IRS to

continue to grow electronic filing remains a good indicator of the stability and capacity of our electronic tax filing system.

Using its adjusted methodology, ETAAC estimates that the e-file rate for individual returns will be just over 89% for the entire 2020 filing season.

Below is an explanation of ETAAC's three-step process to project the full-year electronic filing rate for individual returns for 2020.

……

Step 1: Calculate the actual current year-to-date e-file rate

Determine the current year-to-date e-file rate for individual returns based on actual return filing information through March 6, 2020, which ETAAC calculates to be 95.31%.

Table 3: Tax Year 2019 Individual Income Tax Returns Actual through March 6, 2020

Cumulative statistics comparing 3/8/2019 and 3/6/2020			
	03/08/2019	03/06/2020	**YOY % Change**
Total Receipts	67,721,000	67,998,000	0.41%
E-file Receipts	64,299,000	64,806,000	0.79%
YTD E-file Rate	94.95%	95.31%	0.36%

Source: From "Filing Season Statistics for Week ending March 6, 2020" published by IRS at https://www.irs.gov/newsroom/filing-season-statistics-for-week-ending-march-6-2020

……

Step 2: Estimate historical e-file degradation rate through remaining filing season

In 2020, this step is accomplished by comparing the individual e-file rate through early March with the actual e-file rate for the full-calendar-year filing season for each of the two preceding years – 2018 and 2019. Then, ETAAC uses the average degradation rate experienced over the comparable period for each of the previous two years to forecast degradation for the current year. Using this approach, the e-file degradation rate for the 2020 filing year is forecast to be 6.1%. (ETAAC will continue to monitor the degradation rate to note whether it has any significant year-to-year changes.)

Table 4: Historical Partial-Season Data vs. Full-Season Data

	03/09/18	**11/23/2018**	**Change**	**03/08/2019**	**11/22/2019**	**Change**	**Two Yr. Avg.**
Total Receipts	69,484,000	154,444,000		67,721,000	155,402,000		
E-file Receipts	65,270,000	135,459,000		64,299,000	138,217,000		
E-file Rate	93.9%	87.7%	-6.2%	94.9%	88.9%	-6.0%	**-6.1%**

Source: Various Filing Season Statistics found on www.irs.gov

……

Step 3: Project the full-year e-file rate for individual returns.

Subtract the e-file degradation rate from e-file rate as of March 6, 2020.

Using the IRS's March 6, 2020 data, ETAAC's projected 2020 full-year e-file rate for the individual tax return family is 89.21%. This ETAAC projection is consistent with the IRS's 2020 projection of 90.2% in IRS Publication 6186.

Table 5: 2020 Individual Returns Electronic Filing Projection

	Current @ 3/6/2020	**Avg. Degradation Rate**	**ETAAC 2020 Projection**
Total Receipts	67,998,000		
E-file Receipts	64,806,000		
E-file Rate	95.31%	**-6.10%**	**89.21%**

General Note: Select numeric percentages and results may have slight rounding adjustments.