

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22

ELECTRONIC TAX ADMINISTRATION ADVISORY COMMITTEE

Wednesday, June 27, 2018

9:00 a.m.

The Internal Revenue Service Auditorium

1111 Constitution Avenue, N.W.

Washington, D.C. 20224

1 PARTICIPANTS

2 COUNCIL MEMBERS:

3 JOHN SAPP, Chair

4 DOREEN WARREN, Vice Chair

5 JOHN AMS

6 ROBERT BARR

7 SHANNON BOND

8 LUANNE BROWN

9 ANGELA CAMP

10 JOHN CRAIG

11 JENINE HALLINGS

12 MICHAEL JACKMAN

13 COURTNEY KAY-DECKER

14 SUZANNE KRUGER

15 KATHY PICKERING

16 PHILLIP POIRIER, JR.

17 JOSEPH SICA

18 MARK STEBER

19

20

21

22

| | AGENDA | |
|----|---------------------------------------------------|-------------|
| | <u>PRESENTATION</u> | <u>PAGE</u> |
| 1 | | |
| 2 | | |
| 3 | Welcome | 4 |
| 4 | Remarks | 8 |
| 5 | ETAAC Overview Report and Significant Issues | 11 |
| 6 | Recommendations Review | 42 |
| 7 | Overview of Topic Areas | 42 |
| 8 | Improve IDTTRF Detection, Analysis and Reporting | 46 |
| 9 | Expand and Strengthen the Security Summit and the | |
| 10 | IDTTRF Information Sharing and Analysis | |
| 11 | Center (ISAC) | 46 |
| 12 | Strengthen the Cybersecurity of the Tax Ecosystem | 55 |
| 13 | Enable Electronic Tax Services and Electronic | |
| 14 | Filing | 63 |
| 15 | IRS Comments | 71 |
| 16 | Closing Remarks | 79 |
| 17 | | |
| 18 | | |
| 19 | | |
| 20 | | |
| 21 | | |
| 22 | | |

1 P R O C E E D I N G S

2 MR. HARDY: Good morning. How is everyone?
3 Good. Good. My name is Melvin Hardy. I am the
4 director of the National Public Liaison Office.

5 Welcome to the 2018 ETAAC annual report to
6 Congress. This 2018 report serves as the 19th ETAAC
7 report to Congress. And, just so everyone knows, our
8 Acting Commissioner Kautter is on a tight schedule. So
9 I am going to keep my remarks brief to a couple of
10 points of interest. Unfortunately, he has to leave
11 immediately after his remarks. So the members of ETAAC
12 will quickly assemble themselves to the dais at the
13 very front and get your selfie with Commissioner
14 Kautter. All right?

15 (Laughter.)

16 MR. HARDY: Other than that, like I said, we
17 are on a short timeframe. So I am going to cut my
18 remarks here and introduce the distinguished chair of
19 ETAAC: John Sapp.

20 I will say that ordinarily we are not in this
21 venue, but, as events happen, we were able to secure
22 this great location. So we are very happy to host the

1 ETAAC members and everyone else.

2 I now turn you over to John Sapp. John?

3 CHAIR SAPP: Thank you, Mel.

4 As Mel said, my name is John Sapp. And I am
5 currently the acting chair of ETAAC. We would like to
6 welcome you to the public forum for the presentation of
7 our 2018 ETAAC report. Thank you, Commissioner and the
8 IRS staff for your attendance and your support during
9 our process the past 12 months. It has been an
10 interesting year, to say the least. And I think we
11 have another interesting one coming up.

12 Over the course of preparing our report,
13 ETAAC members have made voluminous requests for data
14 and held numerous meetings and phone calls with various
15 parties within the IRS as well as other partners of the
16 Security Summit. We tried to identify successes and
17 potential areas for improvement in tax administration
18 and efforts to combat ID theft and tax refund fraud
19 with an eye toward the impact on taxpayers; businesses,
20 especially small businesses; as well as state
21 departments of revenue.

22 ETAAC would definitely like to thank those

1 IRS employees and leadership for their continued
2 support of ETAAC. And thank you, Commissioner, for
3 your leadership in this effort. Thank you to Mike
4 Deneroff, who has been both diligent and patient
5 working as our liaison.

6 ETAAC is composed of a diverse membership --
7 most of them are over here -- individuals from the
8 state departments of revenue, private industry, and
9 consumer groups. This diversity allows the IRS to
10 receive a wide variety of perspectives on electronic
11 tax administration and its impact on taxpayers. This
12 year, we welcome back representatives of the payroll
13 community, reinforcing the diversity of our overall
14 team makeup. And several of our recommendations
15 reflect the impact that they have had on our committee.

16 I would like to also thank our committee
17 members. They are volunteers, and they volunteer their
18 time, their knowledge, and their efforts, even though
19 each has a regular day job. They have spent countless
20 hours identifying issues, evaluating solutions to
21 present in this report.

22 I would also at this point like to announce

1 that Doreen Warren, to my right, will become the chair
2 of ETAAC for the next reporting cycle. And we are very
3 excited about her leadership coming the next 12 months.

4 (Applause.)

5 CHAIR SAPP: I would like to especially thank
6 Phil Poirier, who has been a counselor, a scribe, and
7 our chief tail twister --

8 (Laughter.)

9 CHAIR SAPP: -- to make sure we all hit our
10 deadlines in dealing with these issues in our report.
11 We all owe Phil a debt of gratitude for his long nights
12 and weekends, making this report something we are all
13 very proud of. So thank you, Phil. And before you
14 clap, Phil will become the vice chair of ETAAC for the
15 upcoming 12 months. And we would like to congratulate
16 him on that.

17 (Applause.)

18 CHAIR SAPP: Finally, I have to mention
19 Atilla Taluy, who was a member of our ETAAC Committee
20 last year. And he did pass away. He was one of our
21 own. In this past year, he passed away. Those who
22 knew Atilla realized very quickly he was an outspoken

1 advocate for taxpayers and impact this tax
2 administration would have on them. He was a true
3 American success story. He immigrated to America as a
4 young man. He became a rocket scientist, literally,
5 working on the Apollo mission, eventually built a very
6 successful tax software business. He was a respectful
7 calm voice. When debates became chaotic, he was the
8 calm in the storm. He was a friend with a quick smile
9 and a predictable hug for everyone before we could
10 start a meeting. We miss him terribly, and we have
11 dedicated our report to Atilla.

12 So at this point, I would like to hand it
13 over to Commissioner Kautter. And, again, thank you,
14 Commissioner, for your leadership in our efforts.

15 COMMISSIONER KAUTTER: Thanks, John. And I
16 would like to thank everybody on the ETAAC for all the
17 work you have put in this year. All of our advisory
18 groups here at the IRS are important, but I am not sure
19 anyone has a bigger impact than this group, in large
20 part because of your work with the Security Summit.

21 The progress that we have made in
22 cybersecurity is remarkable. As you know, tax-related

1 identity theft is down 65 percent over the last 2
2 years. For 2017, though, we still had 242,000 reported
3 cases of tax-related identity theft. So there is still
4 work to do. And, as we all know, the cyber criminals
5 continue to evolve. And we need to continue to evolve
6 as well.

7 I especially want to thank John for his work
8 this year and Doreen for her work and the willingness
9 to accept the responsibility of the chairmanship next
10 year. This group is in great hands. And, John, you
11 have done a remarkable job. So thank you for
12 everything you have done.

13 The hours that you put in come out of your
14 personal time. You all have full-time jobs for the
15 most part. And I realize that, and we at the IRS
16 realize that. So we are grateful for the amount of
17 effort that you do put into this. Your ideas have been
18 transformational in many respects for cybersecurity
19 here at the IRS. And I was all set to listen to the
20 recommendations this morning, and the Secretary has
21 decided that he has a meeting he would like me to
22 attend at 9:45 on tax reform implementation. And it

1 was, as they say, an offer I could not refuse.

2 (Laughter.)

3 COMMISSIONER KAUTTER: So I have already
4 looked at the report some. I will spend more time with
5 it. You have got some great recommendations. You have
6 done some remarkable work. And I really do want to
7 express my deep appreciation for everything that all of
8 you have done this past year. It really is an
9 impactful group. It is hard for you to see the impact.
10 I think when you are on the Committee, it is hard to
11 sort of look at yourselves through the eyes of others,
12 but you really do make a difference. And so thank you
13 for everything you have done and, as I said, a special
14 thanks to John and Doreen for everything you have done.

15 And, with that, I will turn it back to John.
16 I have got to head out here in a minute.

17 CHAIR SAPP: I think at this time, Mel is
18 going to give us directions. We are going to take a
19 quick break unless you would like to sit and watch the
20 wedding pictures for just a minute.

21 (Laughter.)

22 CHAIR SAPP: You are welcome to do so.

1 MR. HARDY: Could the ETAAC quickly assemble
2 yourselves to the front here with Commissioner Kautter
3 in position? That would be great.

4 (Recess taken.)

5 CHAIR SAPP: Welcome back, everyone. Thank
6 you for your patience as we shuffle and become very
7 flexible in our time together.

8 Just as a point of information, if you would
9 like a hard copy of our report, we have plenty of those
10 out in the lobby. I don't know if "plenty" is the
11 right word, depending on what the demand is like, but
12 there are hard copies of our report in the lobby.

13 So when ETAAC was chartered by Congress in
14 1998, its primary focus was to research and analyze and
15 advise the IRS on achieving a goal to file most major
16 return types, actually all returns, 80 percent of them,
17 electronically. Last year, we estimated the IRS would
18 achieve that goal for major return types and surpass
19 the 80 percent. Of course, our report comes out in the
20 spring, this time of year, and the season doesn't end
21 until November. So that actually ended up being 79.9
22 percent, which you can round up to 80 percent, but

1 technically it was a little short of that 80 percent
2 goal. However, it appears the IRS will surpass that
3 goal to an estimated 81.2 percent, so over a 1 percent
4 margin of error, this year. And we do anticipate they
5 will hit that 80 percent goal. And, again, same as
6 last year, we would like to congratulate the IRS on
7 achieving that monumental benchmark. And that group of
8 returns includes the 1040 and most business returns,
9 including the payroll informational returns. This is
10 ultimately an achievement that benefits the American
11 taxpayer in that e-filing is convenient, cost-
12 effective, and the best way to comply with their tax
13 obligations.

14 One opportunity we are continuing to evaluate
15 is the e-filing of 941 employment returns, where the
16 e-file rate is projected at around 40 percent, which is
17 the lowest among major return types, although the 941
18 on a volume basis is the second highest volume of those
19 return types. So we have made recommendations to the
20 IRS to leverage its public-private relationships to
21 remove any unnecessary barriers to increase e-filing of
22 the 94X series as well as consider reviving the request

1 for agreement of the RFA process to address this issue.
2 It is not the first time ETAAC has made recommendations
3 around the 94X. One of the advantages of having our
4 new payroll members again back on ETAAC was we were
5 able, I believe, to make what I believe is a pretty
6 good recommendation around that volume increase.

7 ETAAC expressed concern last year about the
8 impact of the PATH Act and the delay refund
9 requirements were potentially having on e-file volume
10 and the timing of filing of returns, which at the time
11 had remained static with the prior year or even down
12 just a little. This past year, we experienced a more
13 normal filing season with normal filing patterns and
14 within the 1040 series. And right now it is reflecting
15 a 1 percent increase in the 1040 e-file volume. So it
16 appears to have normalized, although we are still
17 watching that as a process.

18 More recently, ETAAC's charter was expanded
19 to include the ever-changing and urgent issue of ID
20 theft/tax refund fraud, and cybersecurity. As the
21 commissioner mentioned, this is a shift which reflects
22 the ever-changing environment of electronic tax

1 administration. This year, ETAAC continued to focus
2 the majority of our work on the Security Summit and its
3 efforts.

4 In 2015, Commissioner Koskinen and his staff
5 took the extraordinary step of engaging private
6 industry and state governments to form the Security
7 Summit. It is a collaborative effort to fight ID theft
8 and tax refund fraud. This effort has helped protect
9 hundreds of thousands of taxpayers. It has stopped
10 millions of dollars in fraudulent refunds. And our
11 Acting Commissioner Kautter has continued the
12 leadership that Commissioner Koskinen had started. And
13 we would like to thank him again and his staff for the
14 continued leadership to protect both taxpayers and our
15 public funds.

16 So before his exit, I asked Commissioner
17 Koskinen what it was going to take for us to continue
18 the momentum that we had achieved the past few years
19 from the Security Summit efforts. His response was
20 very simple to me, "Continue to provide value to all of
21 the stakeholders." On that note, I will point out the
22 value from the efforts of the Security Summit are

1 pretty clear. In 2017, the IRS saw a 40 percent
2 decline in reports of ID theft from taxpayers.
3 Overall, the number of reported identity theft victims
4 has fallen nearly 65 percent between 2015 and '17. And
5 the number of tax returns with confirmed identity theft
6 declined 32 percent in 2017. Overall, during the 2015
7 to '17 period, that number of confirmed identity theft
8 tax returns fell by 57 percent, with more than \$20
9 billion in taxpayer refunds being protected.

10 The financial industry continued to be a key
11 partner in fighting identity theft and helping the IRS
12 recover fraudulent refunds that may have otherwise been
13 issued, if not identified, by those financial service
14 companies.

15 The value delivered by the Security Summit
16 also goes beyond the numbers on a page. It includes
17 qualitative impact on taxpayers who are able to meet
18 their tax-filing obligations and receive their much-
19 needed refunds, which may have otherwise been delayed,
20 causing a potential financial hardship for many of the
21 most vulnerable taxpayers. However, despite the
22 successes the commissioner mentioned, we cannot relax

1 or assume the threat is decreasing. The American
2 taxpayer is under continuous attack by sophisticated
3 criminals and rogue states, all trying to steal their
4 personal data, which may be used to file false tax
5 returns in their name and receive those fraudulent
6 refunds for criminal purposes. This threat continues
7 to change and is becoming more sophisticated. As a
8 result, the Security Summit must keep pace with an
9 ever-evolving fraudulent activity aimed at
10 misappropriating taxpayer refunds.

11 ETAAC's recommendations are intended to
12 contribute to the summit's evolution and its endurance
13 to outlive any of the individual participants. Of
14 course, Congress' support will continue to play a
15 critical role in that success. So page V of our report
16 has a summary of suggested congressional actions that
17 ETAAC is recommending.

18 Last year, ETAAC made 22 recommendations.
19 The IRS responded to and made great progress on many of
20 those issues, including expanding its outreach to
21 financial institutions, excellent communication
22 campaigns to the taxes' security together, and

1 continuing the ISAC pilot. This year, we have only
2 made 19 recommendations, which I am now going to read.
3 No. Just kidding.

4 (Laughter.)

5 CHAIR SAPP: This year, we have only made 19
6 recommendations, which are summarized beginning on page
7 XI of the report.

8 The report is organized to provide both an
9 overview and a short executive summary and the
10 underlying details of the recommendations in the pages
11 that follow. Doreen Warren will discuss the
12 organization of the report and introduce additional
13 details on our recommendations after our next break.

14 Before I turn it over to Joe Sica, there are
15 two areas in particular that I would like to highlight.
16 First, providing control to taxpayers in a voluntary
17 tax system is a key element. They control, taxpayers
18 control, when they file; how they file; how their
19 refund is disbursed; and, to a large degree, if they
20 must file a tax return. Our recommendation number 18
21 is around the account lock and unlock, provides
22 additional control within that process for a taxpayer

1 in filing their tax return. Essentially, the
2 recommendation is that a taxpayer, similar to the way
3 they may do their credit report, they can log into
4 their account and lock it so that no return can be
5 filed on their account and then make a decision to
6 unlock it before they file their tax return. We know
7 that this recommendation has been made by other
8 parties, the Taxpayer Advocate and IRSAC, for example,
9 and ETAAC adds its voice to that chorus to have the IRS
10 implement that recommendation.

11 In addition, along with that control, we have
12 recommended the IRS should extend eligibility to obtain
13 an IP PIN, or identity protection personal
14 identification PIN, to all individual taxpayers.

15 And, second, the expansion of the summit to
16 include additional members of the tax ecosystem,
17 especially the payroll community, will continue to
18 address the pipeline of fraud detection and prevention.
19 If you think about the pipeline of tax filing, it ends
20 up with the money going into a taxpayer's bank account,
21 but it starts with the issuing of the source documents,
22 such as the W-2's that most taxpayers will utilize to

1 file their tax returns. So having the payroll industry
2 involved in that process is essential to validate that
3 source documents. Are they accurate source documents
4 that pertain to the taxpayer that is filing the tax
5 return? So the IRS has made efforts in that, and we
6 applaud that. And one of our main recommendations is
7 they continue that effort to do so.

8 So in terms of the rest of our meeting
9 structure, I will point out after the break some of our
10 braver ETAAC members, who will provide an overview and
11 more details on specific recommendations for future
12 actions. We also have recommendations in the area of
13 ETAAC's traditional focus: the electronic filing and
14 online services that I mentioned before.

15 ETAAC efforts are led by subgroups, which
16 mirror the structure of the Security Summit. So before
17 we turn over to our specific recommendations, we would
18 like to review the progress of the Security Summit
19 working groups and the ISAC to date. To do that, I am
20 going to ask our three subgroup leaders to review some
21 key recent activities in their areas of responsibility.
22 And, just to get the overview of that, the filing

1 subgroup is led by Joe Sica. And that supports the
2 Security Summit's authentication and financial services
3 workgroups. The sharing subgroup is led by Mark Steber
4 and supports the info-sharing and ISAC. And the
5 outreach subgroup is led by John Ams and supports the
6 tax pros and communications workgroups. I didn't get
7 the last copy printed.

8 And at this time, I would like to turn it
9 over to Joe Sica.

10 MR. SICA: Thanks, John.

11 Hi. My name is Joe Sica. I am the chief
12 public policy officer for Green Dot Corporation,
13 primarily focused where their business relates to tax-
14 time financial product offerings. As the filing
15 subgroup leader, however, my team is focused on the
16 activities of three Security Summit workgroups. The
17 first is the authentication workgroup, which is tasked
18 with strengthening authentication by finding new ways
19 to validate taxpayers and tax return information.

20 Next is the Strategic Threat Assessment and
21 Response workgroup. You may have heard it referenced
22 by its acronym: the STAR working group. This group is

1 tasked with addressing identity theft/tax refund fraud
2 points of vulnerability and has the unenviable but very
3 critical focus on enhancing the cybersecurity across
4 the tax ecosystem. It is a very highly technical group
5 for sure.

6 The last group the filing subgroup is focused
7 upon is the financial services working group, which is
8 tasked with finding ways to leverage the financial
9 services industry to identify and block identity
10 theft/tax return fraud refunds, and prevent criminals
11 from using financial products to enable their crime
12 schemes. The group also focuses upon enhancing the
13 suspect leads process that if acted upon quickly enough
14 don't allow criminals to abscond with the funds which
15 are, in turn, returned to the IRS or the appropriate
16 state's department of revenue.

17 These three working groups have undertaken
18 several initiatives to strengthen the Security Summit
19 itself; improve cybersecurity; and enhance identity
20 theft/refund fraud detection, analysis, and reporting.

21 For instance, the authentication workgroup
22 continues to implement trusted customer requirements to

1 improve IRS and state ability to identify suspicious
2 returns and reduce instances of identity theft/tax
3 refund fraud. They are also expanding authentication
4 initiatives to protect business taxpayers and blunt the
5 current expansion of identity theft/refund fraud
6 criminal activity in the business returns.

7 The STAR workgroup continues to develop and
8 implement security controls of the NIST cybersecurity
9 framework standards, working directly with industry tax
10 software and e-filing companies. They are also
11 expanding their engagement beyond income tax companies
12 and widening their cybersecurity net to payroll and
13 employment tax companies.

14 The financial services working group has
15 increased the number of financial services providers
16 participating in the federal and state external leads
17 program. They have also collaborated with industry to
18 leverage the unique capabilities of financial service
19 companies, such as its pre-validation pilot intended to
20 identify suspicious refunds before IRS or the states
21 release refund direct deposits. So, instead of
22 following the money, using a secured access to inquire

1 against the intended financial institution's account
2 authentication database, the group is working on
3 strategies that will help stop suspect funds from
4 initially leaving the revenue agencies so they can be
5 further reviewed for fraudulent activity.

6 But if I had to identify one big issue in
7 these areas, I would say it is how to integrate new
8 industries and other government agencies into the
9 Security Summit in the most effective and efficient
10 way. Somewhat treated as cliché at times, the public-
11 private collaboration model cannot be underestimated
12 and lost sight of. The Security Summit and its
13 successes are an example where when serious and trusted
14 stakeholders of both government and private sector
15 combine various technical expertise problems like
16 identity theft/tax refund fraud are attacked
17 effectively and efficiently, if not more economically.

18 Obviously, we are all smarter together. And
19 the reduction of related identity theft/tax refund
20 fraud three years running has saved the government
21 billions of dollars while mitigating disruption to the
22 American taxpayers' filing experience, who, selfishly,

1 are also industry's customers. To help illustrate this
2 reduction that has been previously stated, overall, IRS
3 reports the number of identity theft victims has fallen
4 nearly 65 percent between 2015 and 2017.

5 And also as previously stated but I think
6 very astonishing and cannot be underscored enough,
7 overall during the same period, the number of confirmed
8 identity theft/tax refund tax returns fell by 57
9 percent, with more than \$20 billion in taxpayer refunds
10 being protected. I think that is amazing. So fraud is
11 nobody's friend. And collaboration attacking it has
12 proven to be a triple win, recipe for government,
13 industry, and the taxpayers we both serve, but the work
14 is far from finished.

15 For example, criminals are targeting payroll
16 companies to steal employee data to enable identity
17 theft/tax refund fraud schemes. The result is it is
18 getting increasingly more difficult to filter out
19 fraudsters from legitimate taxpayers and customers.
20 Therefore, trending false positive rates on previously
21 proven fraud deterrents are troublesome.

22 We also find that criminals are getting more

1 patient. They are setting up fraudulent financial
2 accounts long in advance of tax season and will
3 transact in them for some period of time in an effort
4 to make the account less likely to get caught in
5 suspicious activity filters at tax refund time.

6 And, finally, evidence shows that many of the
7 same stolen identity data is showing up on payments
8 made by the Social Security Administration, the
9 Veterans Administration, and FEMA.

10 These few examples illustrate that the IRS'
11 and the summit's jobs are far from done as criminals
12 become more sophisticated and innovative.

13 The IRS also reports that the financial
14 industry is a key partner in fighting identity theft,
15 helping the IRS recover fraudulent refunds that may
16 have been issued. In that same time period, 2015
17 through 2017, banks helped recover over 517,000 suspect
18 refunds, totaling \$1,337,000,000. So while the IRS has
19 definitely strengthened relationships to combat fraud
20 with the agencies I just mentioned previously, imagine
21 the value of now adding the financial institution
22 experience in identifying suspect payments beyond just

1 IRS refunds. So only by continuing to collaborate and
2 widen the net with organizations outside the
3 traditional tax base will IRS, states, and industry
4 have a chance to keep pace with the fraudsters. It
5 will be critical to understand the differences and
6 similarities of these non-tax entities so that they can
7 be integrated into the Security Summit initiatives in
8 the most effective manner. Our 2018 report will have
9 some specific recommendations concerning these issues
10 as well as increasing member participation in the
11 summit, specifically the STAR working group, and
12 establishing a common security standard.

13 Unless commissioner -- oh, no. I shouldn't
14 read this part. I guess he doesn't have any comments.
15 He is not here.

16 (Laughter.)

17 MR. SICA: So I would like to hand off to
18 John Ams now, the outreach subgroup leader. Sorry
19 about that.

20 MR. AMS: Good morning, everyone. My name is
21 John Ams. In my day job, I am the executive vice
22 president of the National Society of Accountants. But

1 I am here today as the outreach subgroup leader.

2 Our group focused on the identity theft
3 issues faced by taxpayers on a daily basis as well as
4 the hundreds of thousands of tax professionals whose
5 data and clients are prime targets for identity theft.
6 Our goal was to continue to create awareness in the
7 hope that this would also lead to action.

8 My team is focused on the activities of two
9 Security Summit workgroups: the communications and
10 taxpayer awareness workgroup, which is tasked with
11 increasing awareness among individuals, businesses, and
12 tax professionals on the need to protect sensitive data
13 and financial information. We also looked at the tax
14 professional workgroup, which is tasked with examining
15 the impact of Security Summit initiatives on the tax
16 professional community and how that community can
17 contribute to the prevention of identity theft.

18 Let me first point out some of the impressive
19 progress made over the last year by highlighting just a
20 few of the initiatives undertaken by the workgroups in
21 my areas of responsibilities. The communications
22 workgroup was very active. And I do want to thank

1 Terry Lemons for all of his efforts in this regard. It
2 has been outstanding. That group conducted the "Don't
3 Take the Bait" national tax security awareness week,
4 which included developing and issuing numerous news
5 releases and tax tips to guide individual and business
6 taxpayers on steps to protect their tax data and
7 identities. And that took place in advance of the 2018
8 filing season. They also worked with state and private
9 sector Security Summit partners, local consumer groups,
10 law enforcement agencies, and other government groups
11 to conduct over 30 different events across the country.
12 They continued taxpayer awareness campaigns, such as
13 tax securities, together. They also expanded security
14 awareness campaigns of tax professionals with the
15 "Protect Your Clients. Protect Yourself" campaign to
16 raise awareness among tax professionals about their
17 legal obligation to protect taxpayer data and to
18 highlight the security risk posed by identity thieves.

19 Meanwhile, the tax professional workgroup
20 worked behind the scenes in collaboration with numerous
21 stakeholders in the tax community to create some of the
22 suggestions and tax tips used in outreach efforts.

1 Their efforts resulted in the publication of actionable
2 guidance to tax professionals interested in making
3 their offices and their data files more secure from
4 cyber criminals. This included guidance on situations
5 such as what to do when a tax professional sells or
6 shuts down their tax practice. For example, what steps
7 should be taken during the sale or transfer to ensure
8 secure data?

9 The workgroup also developed suggestions for
10 tax professionals who have experienced a data breach,
11 including what should be reported, to whom should any
12 information be reported, what should next steps be. As
13 IRS statistics made clear, however, tax professionals
14 are increasingly being targeted by cyber criminals.
15 Consequently, the one area I would like to focus on is
16 the need to assemble a clear security standard for tax
17 professionals. And related to that, we need to give
18 the IRS the authority to enforce that standard.

19 First, make no mistake. A security standard
20 was first established in 1998, when the Gramm-Leach-
21 Bliley Act was enacted. But that standard, the so-
22 called safeguards rule, was meant for all businesses

1 that deal with consumers. It was not specifically
2 designed for taxpayers who have confidential data that
3 they are required to transmit electronically. This
4 raises different security risks than those faced by
5 businesses that merely stored data that they may get in
6 the course of a consumer buying a product. In any
7 event, Gramm-Leach-Bliley specifically made that
8 security standard applicable to tax return preparers
9 but left enforcement up to the Federal Trade
10 Commission, not the IRS. This raises the question
11 whether the IRS has the authority to initiate any
12 enforcement activity for violations of the safeguards
13 rule or whether the IRS can act only after the FTC has
14 a found a violation of that rule.

15 Although the FTC has published a number of
16 very useful tips for businesses subject to the rule,
17 sometimes in conjunction with the IRS, we are aware of
18 only one enforcement action initiated by the FTC for a
19 safeguards rule violation by anyone in the tax
20 professional community, and that is after 20 years.

21 Furthermore, we were advised that due to the
22 definition of consumer in Gramm-Leach-Bliley, the

1 preparers covered by the safeguards rule may only be
2 those serving individuals, not businesses. Given that
3 cyber criminals are increasingly targeting businesses
4 because that is where the money is, that is very
5 concerning from a tax system security viewpoint. So it
6 seems that although there is a security standard, it
7 may not be applicable to business return preparers, and
8 it is also unclear whether a violation of that security
9 standard is subject to enforcement by the IRS. We
10 believe taxpayers deserve better. After all, it is
11 their identity and money that is being stolen.
12 Something better would be a clear and enforceable
13 security standard applicable to all tax professionals,
14 whether they are acting as a tax adviser, a consultant,
15 a return preparer, a payroll professional, transmitter,
16 or in any other capacity that gives them access to
17 confidential taxpayer data.

18 We also want to make clear that the term "tax
19 professional" is more than just tax preparer. Frankly,
20 not knowing how to properly prepare a return to even
21 being unaware of the difference between the Internal
22 Revenue Code and the Da Vinci Code is not the point.

1 This is about preventing the theft of confidential
2 data, no matter who in the tax ecosystem is holding
3 that data. As we know, tax return preparers are only
4 part of this tax supply chain. The electronic
5 submission of a tax return may involve individuals or
6 entities whose only role is to take a return from the
7 preparer or even directly from the taxpayer and
8 transmit it to the IRS. As I have said, at best, it is
9 unclear whether the return transmitter is subject to
10 the safeguards rule because there is no return
11 preparation involved at all. We believe that it is
12 time to have a clear and enforceable standard,
13 enforceable by the IRS.

14 Our 2018 report has some specific
15 recommendations concerning outreach and strengthening
16 the security capabilities of tax professionals. I
17 encourage you to read the report in its entirety.

18 I would now like to call on Mark Steber,
19 ETAAC's information-sharing subgroup leader.

20 MR. STEBER: Good morning. My name is Mark
21 Steber. I am the chief tax officer for Jackson Hewitt.
22 And, as John and John and others have mentioned, I am

1 also the information subgroup leader. My team is
2 focused on two principal security subgroup components.
3 The information-sharing workgroup, which is tasked with
4 identifying opportunities for sharing information to
5 improve the collection capabilities for information for
6 detecting and preventing tax ID theft and tax refund
7 theft. We also have, you know, interaction in working
8 with the Information Sharing and Analysis Center,
9 commonly known by its acronym the ISAC, which is tasked
10 with centralization, standardization, and enhancing
11 data compilation analysis to identify actionable ideas
12 and actionable activity for tax refund/identity theft
13 fraud as well. It includes sharing with alerts to the
14 system and the overall ecosystem to protect taxpayers
15 and their data.

16 As did Joe and John, let me point out a few
17 of the initiatives and successes for both the
18 information-sharing working group and for the ISAC for
19 the year. First, a little bit of background. The
20 information-sharing workgroup had from its start as one
21 of the original security workgroups to identify and
22 collect information, information outside of the regular

1 taxpayer filings for use with identification and
2 prevention of tax refund fraud and tax refund theft to
3 verify bad tax returns and key indicators within tax
4 returns that would help the entire system prevent some
5 of the attacks from tax refund fraud, to identify
6 schemes and share that information.

7 One of the principal functions of the working
8 group was to identify select data each year, have tax
9 industry members collect that data, and forward that
10 information on over to the IRS. In part, as part of
11 that activity, it would also collect leads, you know,
12 verified and suspicious tax return activity, share that
13 information with the IRS. And then the IRS would share
14 that broader with the overall system so that we could
15 get in front of some of these schemes faster and more
16 effectively than we have in the past. So from the
17 start, the information-sharing working group was
18 working to gather information, to collect that
19 information. And by its very name, to identify
20 information that we could collect and reinforce the
21 protections to taxpayers and their tax refunds
22 enterprise-wide and beyond.

1 This year was another successful year with
2 greater improvement to the data collected, greater
3 refinement of the data elements that we look at and the
4 use of those elements, and enterprise-wide leverage of
5 that information.

6 The leads process also worked equally well
7 during the year. Information was collected for W-2
8 schemes, state schemes, a variety of other schemes, and
9 shared with the industry in the prevention and
10 mitigation of tax refund fraud. As I say, several
11 schemes were identified at the front end and worked to
12 be prevented enterprise-wide and scaling up higher than
13 in years past, overall a very successful year from
14 information sharing and collection and processing.

15 The ISAC, also a very successful year. A
16 quick, brief history for those of you who are not
17 familiar with an ISAC and what it does, by its very
18 definition, the ISAC is an information sharing and
19 analysis center. So they take collectively
20 information. They analyze it. They identify issues
21 that can be acted on. And then they share that
22 information with stakeholder partners. There are, of

1 course, ISACs for banking, for air travel, for medical
2 services, and virtually every large industry. The ISAC
3 for taxes is no different. And, by its very name, it
4 analyzes data and shares that data for the collective
5 good of the industry, in our case, the prevention of
6 tax refund fraud.

7 The ISAC for our tax industry is managed
8 through a partnership with an independent third party,
9 the MITRE organization, and administered by the IRS in
10 partnership with the tax industry, states, and other
11 stakeholder members, each having representative
12 membership.

13 The ISAC, of course, is in the second
14 successful pilot year and from all accounts was very
15 successful. We would like to thank Todd for being here
16 today, and I am sure he will share some other
17 information with us later.

18 Wins for the past season include continued
19 expansion of members. As Joe had mentioned, the
20 outreach has been very successful in getting many more
21 states to be a participant to the ISAC and more
22 industry members coming on board every day

1 Several alerts were posted during season real
2 time that helped us as industry members get in front of
3 a variety of sophisticated and far-reaching tax schemes
4 and, again, by very definition, a very successful year.

5 In summary, the Information Collection and
6 Analysis Center and the information-sharing group had
7 worked to get data, to share that data, to leverage
8 that data. However, there are still some shortfalls.
9 Information collecting was the precursor to the ISAC.
10 And now the ISAC has come on board as the next logical
11 step. Collecting information, analyzing the
12 information, reporting out through reports and alerts
13 to the system on where they might prevent activity from
14 happening.

15 The ISAC was the natural evolution of the
16 information sharing and the next step for processing
17 data and leading to preventive maintenance, including
18 the leads process, as we have used in years past. And
19 it also provides feedback to the system and to other
20 ISACs. But with the information about the conclusion
21 of the collections data and the information sharing
22 over the past few years, a more accurate data

1 collection process is probably needed.

2 Having said that, what is still short in the
3 law are certain limitations for information sharing.
4 Due to current laws, regulations, and historical
5 practices, there are limitations on how data and
6 information can be fully utilized.

7 For example, known and verified data, such as
8 a fraudulent bank account number used for suspicious or
9 even fraudulently verified activity, is currently
10 prohibited from being shared throughout the system,
11 even though it has been proven to be false. And so
12 there may be some improvement areas available to
13 further allow the utilization of data that we currently
14 collect and the refinement of that data to promote and
15 expand prevention efforts.

16 Current law has certain legacy safeguards --
17 and we recognize those -- and well-intended limits to
18 prevent how certain data can be fully leveraged, but we
19 think there might be a better way. So full use of
20 known and suspicious data is currently being used but
21 could perhaps be expanded. And, as Joe and John said,
22 if I had one area that I would focus on during the

1 report, I would say it is how we can move to the next
2 iteration or the next level on sharing information to
3 help us better analyze and identify tax refund theft
4 schemes. One opportunity is this area to modify
5 existing legislation and permit appropriate and safely
6 sharing information used to fight sophisticated and
7 ever-expanding refund crime schemes. The ability to
8 more broadly share and leverage protected data is the
9 next logical step for these two important groups, the
10 information-sharing group and the ISAC group, to move
11 forward and prevent greater tax refund fraud.

12 Our 2018 report has some specific
13 recommendations to enable information sharing and
14 enhance our ability to identify and communicate
15 schemes. More and more members, more and more industry
16 players and tax ecosystems are participating. And it
17 is important to go to the next level and utilizing the
18 information that they will bring to bear but using it
19 carefully and well-managed as we go forward.

20 At this point, I will hand it back to John
21 for some closing comments and a short break. And then
22 we will move into some of the detailed recommendations

1 by some of our ETAAC members, who can speak more
2 diligently to the specifics within the report. John?

3 CHAIR SAPP: So, with this, right before we
4 go into our break, I will see if anyone from the IRS
5 has any comments at this point. Obviously we have a
6 section toward the end of our -- after we do more
7 detailed recommendations for the IRS to comment. But
8 does anyone -- Terry, do you --`

9 MR. LEMONS: Right. And our leaders on the
10 IRS side will have some more to say I think later on as
11 we get into more specifics, but, you know, just on
12 behalf of the commissioner and all of IRS, I just want
13 to thank ETAAC for the very detailed report. Last
14 year, I know Mike, Todd, Ed, and the other members
15 active with the Security Summit effort, we spent a lot
16 of time looking at the ETAAC report. This is not a
17 report that just goes up on a shelf and, you know,
18 nothing happens with it. We viewed it as a, you know,
19 valuable tool. And from our standpoint, this was a
20 great example of how the advisory committee process
21 works. So the group, the ETAAC group, has made a great
22 contribution to helping us run the nation's tax

1 administration system. So I really appreciate all of
2 the hard work and effort by the members. And we will
3 have some more specific comments later on.

4 CHAIR SAPP: Okay. Great. At this time, we
5 are a little ahead of our schedule, which is really
6 good news and not that usual. We have probably thrown
7 some of our ETAAC members off that were running ahead.
8 So we will take a quick break. And we will reconvene
9 at 10 o'clock. So that gives us about 15 minutes to
10 break. Let's do that. And we will reconvene right at
11 10 o'clock. And then we will have about another hour
12 worth of content as we go through our recommendations.
13 Thank you.

14 (Recess taken.)

15 VICE CHAIR WARREN: As soon as Joe takes his
16 seat, we will go ahead and get started.

17 CHAIR SAPP: So at this time, I would like to
18 introduce Doreen Warren.

19 VICE CHAIR WARREN: I wasn't expecting you to
20 do that.

21 CHAIR SAPP: We are extremely fortunate to
22 have Doreen, who is one of the most articulate

1 advocates for the state departments of revenue.
2 Although she comes from probably what would be
3 considered a smaller, population-wise, state, the State
4 of Idaho, Doreen speaks with a very active voice in all
5 of the Security Summit efforts and is very thoughtful
6 and understands the issues that affect not only state
7 departments of revenue but how those interact with the
8 entire tax system from the IRS all the way through to
9 tax transmitters, tax preparers. Doreen spends time
10 meeting with tax preparers. She gets out, and she
11 spends less time in her office probably than I do.

12 So at this time, we will turn it over to
13 Doreen Warren.

14 VICE CHAIR WARREN: Well, thank you, John.

15 Good morning. And welcome back from the
16 break. What John failed to say is that I am just never
17 short of opinions.

18 (Laughter.)

19 VICE CHAIR WARREN: And I have been with the
20 Security Summit since its very beginning. So it has
21 been a very rewarding experience to be participating in
22 that.

1 As John said, my name is Doreen Warren, and I
2 am currently the public information director for the
3 Idaho State Tax Commission and also currently serving
4 as the ETAAC vice chair.

5 The IRS Security Summit has made a
6 significant contribution protecting taxpayers in
7 innovative and collaborative ways. We as ETAAC
8 recognize the IRS' leadership and the many capable,
9 thoughtful, and committed IRS employees assigned to the
10 IRS Security Summit and ISAC initiatives. There is
11 also no doubt that coordinating the efforts of such a
12 diverse stakeholder group presents a few challenges.
13 And the IRS has done a remarkable job of engaging with
14 both state departments of revenue and a broad range of
15 private sector stakeholders. And at this point, they
16 actually recognize the states as a partner, and that
17 has been very rewarding as well.

18 As a representative from the state department
19 of revenue, I can say that we are seeing similar
20 results and trends as the IRS is seeing. While the
21 states are witnessing an overall reduction in confirmed
22 fraud, we are also seeing an increase in tax

1 professional breaches and business fraud.

2 With all of the good effort and the
3 accomplishments made to date, there is still more work
4 to be done. We have heard that both from Commissioner
5 Kautter and from John as well. IRS' continued
6 leadership coupled with its ability to coordinate and
7 facilitate diverse partnerships will continue to be a
8 critical competency for the success of the Security
9 Summit in electronic tax administration.

10 So before we dive into the recommendations, I
11 would like to share a few key points. We have heard it
12 this morning, but it is worth repeating. First of all,
13 the Security Summit under the IRS' leadership continue
14 to make progress in the fight against identity
15 theft/tax refund fraud. And this threat will never
16 end. Criminals are constantly adjusting their
17 strategies and tactics to find ways to steal individual
18 and business identities and convert those stolen
19 identities into tax refunds.

20 The IRS, states, and industry have made a
21 strong commitment of resources to the Security Summit.
22 The congressional funding and support remains a key

1 enabler. The Security Summit must continue to expand
2 its scope and the level of membership participation as
3 well. And, finally, success in cybersecurity is a
4 moving target. It requires continuous innovation and a
5 forward-thinking mindset.

6 So let's talk about our recommendations for
7 this year. The primary focus in the 2018 report to
8 Congress continues to be on protecting taxpayers by
9 suggesting methods and processes to fight identity
10 theft/tax refund fraud and enhancements to the security
11 of our electronic tax infrastructure. Our report also
12 provides recommendations for the Internal Revenue
13 Service to increase electronic filing and expand
14 electronic services.

15 Before the break, you heard from each of the
16 subgroup leaders about progress that has been made and
17 one big issue within each area. We are now going to
18 hear from those brave team members that John mentioned
19 earlier to hear an overview of the specific
20 recommendations for future action within each area. We
21 will provide an overview of each of the
22 recommendations. We are not reading the detailed

1 recommendations. We will leave that for you as you go
2 through the book. The summary of the recommendations
3 begins on page 11. And the detailed recommendations
4 begin on page 14.

5 The principal recommendations in 2018
6 generally fall into 4 broad categories: the first one,
7 expand and strengthen the Security Summit and the
8 identity theft/tax refund fraud Information Sharing and
9 Analysis Center, also known as the ISAC; the second
10 area, strength the cybersecurity of the tax ecosystem;
11 third, improve identity theft/tax refund fraud
12 detection, analysis, and reporting; and, finally,
13 enable electronic tax services and electronic filing.

14 So, to begin, I will hand it over to Kathy
15 Pickering, who will discuss our first set of
16 recommendations. Thank you.

17 MS. PICKERING: Thanks, Doreen. Appreciate
18 that.

19 I am Kathy Pickering. I am the executive
20 director of the Tax Institute at H&R Block.

21 I am going to provide an overview of the
22 recommendations focused on improving identity theft

1 detection, analysis, and reporting, which are
2 recommendations 11, 12, and 13. If you are following
3 along with the agenda or with the report, you will
4 notice I am going slightly out of order. So don't let
5 that throw you.

6 So the ability to share information across
7 the tax ecosystem about suspicious activity and
8 identity theft is essential to successfully fighting
9 identity theft/tax refund fraud. With the
10 implementation of the ISAC, the tax industry and the
11 states have been able to share information amongst
12 themselves about suspicious patterns and trends.

13 Currently, there are limitations on IRS'
14 ability to share identity theft information,
15 specifically with the tax industry. IRS section 6103
16 is designed to protect taxpayers with carefully defined
17 conditions on the use and disclosure of return
18 information by the IRS. These limitations, however,
19 constrain the effectiveness of information sharing for
20 fighting identity theft/refund fraud. Section 6103
21 provides important protections around taxpayer
22 information. ETAAC believes those protections can be

1 maintained while at the same time creating an exception
2 for its use and disclosure by the IRS to prevent and
3 detect identity theft/tax refund fraud. To that end,
4 recommendation number 11 encourages Congress to enact a
5 carefully defined fraud exception under 6103. Our
6 report even offers principles that could be used to
7 define how the regulations would be implemented to
8 ensure the appropriate balance of taxpayer
9 confidentiality and identity theft/tax refund fraud
10 protection.

11 Our report also raises the issue of increased
12 criminal activity associated with business returns,
13 such as fake business identities filing false returns.
14 You will notice in the report there is an outstanding
15 statistic that for form 1120, confirmed fraud, the
16 average refund claimed was \$1.3 million. IRS and state
17 revenue agencies have had some success in
18 authenticating returns because of additional
19 information included in the electronic return.
20 Recommendation 12 builds on this foundation by
21 recommending that the IRS continue to work with the
22 Security Summit to enhance the data elements in the

1 business e-filing schema and assess the benefits and
2 effectiveness of business leads reporting. The IRS has
3 already begun working in this area, and we support
4 that.

5 Finally, as mentioned, tax preparers and tax
6 return filers play a critical role in our tax system.
7 Two of the key identification mechanisms are the
8 electronic filing identification number, or the EFIN;
9 and the preparer tax identification number, or the
10 PTIN. The EFIN is the number associated with the
11 physical location that files tax returns. Some
12 fraudsters have been able to commandeer EFIN
13 credentials and file false returns under a legitimate
14 EFIN, making it more difficult to detect fraud
15 activity. Similarly, fraudsters have filed returns
16 under false PTIN credentials. Additionally, legitimate
17 returns can be filed under expired or invalid PTINs.
18 The tax industry can play a more proactive role, even
19 before the start of the filing season, if there is an
20 ability to validate these numbers, the EFINs and the
21 PTINs, in real time using up-to-date IRS databases.
22 Number 13 recommends that the IRS creates mechanisms to

1 enable approved third parties to validate EFINs and
2 PTINs in real time to help protect the integrity of our
3 tax system.

4 Next, I am going to hand off to Jenine
5 Hallings to discuss the next set of recommendations.

6 MS. HALLINGS: Good morning. Thank you. My
7 name is Jenine Hallings, and I work currently for
8 Paychex, Incorporated. I have been there 22 years.
9 And for those of you that are familiar with Paychex, we
10 are a payroll service provider that services over half
11 a million small- to medium-sized businesses nationwide.
12 My role is in the area of risk management. And I am
13 going to talk to you this morning a little bit more on
14 recommendations 1 through 4 in the annual report and
15 really try and share with you why payroll is such an
16 important area of focus in combating fraud within the
17 context of the overall tax ecosystem.

18 So when you think about the type of data
19 fraudsters are looking to get their hands on, that
20 personally identifiable information, that type of data
21 is exactly what is captured in payroll. Payroll is
22 really the starting point of tax data entering into the

1 ecosystem. And it brings us to our first
2 recommendation in the report, and that is to integrate
3 the payroll community more broadly into the Security
4 Summit and the Information Sharing and Analysis Center.

5 The payroll community is quite diverse. Not
6 only does it include large and small payroll providers,
7 but it also includes individual employers who file
8 their own employment tax returns. However, what we all
9 share is that vulnerability to fraud if we let our
10 guard down.

11 So what I want to share with you just as an
12 example of one of the more common schemes we saw in the
13 payroll community, we had fraudsters out there
14 pretending to be someone from the company's HR
15 department and actually asking the CEO in an email to
16 send copies of the employees' W-2's as soon as
17 possible. And I know that was something that was
18 communicated out through the Security Summit. You
19 know, that was a really simple but effective scheme for
20 fraudsters to deploy. You know, the success wasn't
21 really dependent on whether the business was large or
22 small, but, really, the best defense against that was

1 awareness to the scheme. And that was the fact that
2 that fraud trend, in particular, was on the rise.

3 The other way to kind of look at that scheme
4 is to look at it as a first step in a more complex
5 fraud that enables a fraudster to gain access to
6 valuable PII that they need. Increasingly, we are
7 seeing this PII being leveraged in schemes of greater
8 complexity, and that is a very concerning trend. The
9 more data that the fraudster accumulates on an
10 individual or business just increases the likelihood of
11 them being able to identify a way to circumvent fraud
12 detection filters and steal tax refunds or tax
13 identities.

14 So this is what makes the payroll community's
15 involvement in Security Summit and ISAC so critical.
16 The Security Summit and the Information Sharing and
17 Analysis Center are well-positioned to facilitate the
18 sharing of information across the payroll community in
19 a more streamlined manner.

20 Recommendation 2 is really surrounding an
21 increased outreach to employers and businesses in
22 collaboration with the Security Summit. You know, it

1 is important to be mindful of threats evolving in other
2 parts of the tax ecosystem. Employers are increasingly
3 becoming a target of identity theft, as you have heard,
4 as a recurring theme in a lot of the comments so far
5 this morning where the fraudsters steal the employer's
6 identification number in the execution of their scheme.
7 Outreach by the IRS via the Security Summit in their
8 communication campaigns is really a valuable tool that
9 can be leveraged even more robustly to educate
10 employers in guarding against fraudulent activity. It
11 can be a useful channel of communication to provide
12 clear and simple reminders of how to report a fraud if
13 one has occurred.

14 Now I want to focus a little bit of attention
15 on recommendation 3 in the report, and that is centered
16 around ensuring the effective operations of the
17 Security Summit. We recommend the creation of
18 documentation that explains the purpose, the
19 responsibilities, and the goals of the Security Summit
20 as well as the ISAC working groups. Over the course of
21 time, we feel it is reasonable to expect there will be
22 turnover as people change jobs or a new member joins.

1 And we want that ramp-up period to be as efficient and
2 quick as possible. Documentation that captures work
3 flows, that will help minimize the loss of knowledge
4 that is brought about by turnover will be a valuable
5 tool to assist in this. You know, reference material
6 is also going to be able to help the facilitation of
7 on-boarding new members that rotate in.

8 The final recommendation, number 4, that I am
9 going to be speaking to this morning is how critical we
10 believe it is for the IRS to continue to enable
11 collaborative innovation. So there are a lot of
12 examples already of public-private partnership in tax
13 preparation, for example, the VITA and TCE program.
14 Free file would be another example. And the Security
15 Summit itself is a platform for collaboration. You
16 know, we believe it is tremendously valuable in looking
17 at an issue comprehensively from a variety of
18 perspectives. You know, fraud is such a pervasive
19 problem today. And how it impacts the payroll
20 community might be slightly different from how it is
21 impacting another portion of the ecosystem. But being
22 mindful of this further supports the need for

1 collaboration and greater understanding because it is
2 no longer an environment where, you know, we can defend
3 ourselves alone. It really is requiring folks to come
4 together, have a little bit of trust in the fight
5 against fraud.

6 Now I would like to turn over the podium to
7 Phil. And he is going to take us through the next
8 grouping of recommendations. Thank you.

9 MR. POIRIER: Thank you, Jenine.

10 My name is Phil Poirier. I am a senior
11 fellow with the Center for Social Development at
12 Washington University in St. Louis as well as a VITA
13 volunteer.

14 Before I jump into reviewing the
15 recommendations that I am going to cover, I just want
16 to reinforce some things that have already been said
17 about IRS' progress in this area. I would love to call
18 out the individual employees we have all worked with
19 over the past few years, but we would miss people. The
20 level of capability and commitment and creativity of
21 the IRS employees, managers, and leaders working on
22 this as well as from industry and from the state

1 departments of revenue is very encouraging. And the
2 progress to date is reflecting those aspects.

3 I am going to focus on our six
4 recommendations relating to the strengthening of
5 information in cybersecurity. These are
6 recommendations 5 through 10.

7 As you have already heard, several speakers
8 have mentioned how criminals are expanding their
9 targets into the business tax return system, which
10 would include payroll, as well as targeting tax
11 professionals. We believe that there are opportunities
12 to enhance the protection by taking actions in both of
13 these areas. In many cases, we are talking about
14 building upon steps that IRS is already taking. In
15 other cases, they might be new twists or turns.

16 There are two broad categories for the
17 recommendations I am reviewing. One category is
18 establishing common security standards and practices,
19 and the second category is improving the security
20 posture of tax professionals. So we are going to start
21 with the first category: establishing common security
22 standards and practices.

1 John Ames has already described the Gramm-
2 Leach-Bliley Act, or GLB; and the FTC safeguards rule,
3 which was issued by the Federal Trade Commission under
4 that legislative authority. The safeguards rule is
5 very basic and very simple. As a standard, all it says
6 is you need to have an information security program,
7 you need to have designated information security
8 personnel, you need to conduct a risk assessment, and
9 you need to design and implement information safeguards
10 that are appropriate to your business. That literally
11 is the substance of the FTC safeguards rule. It is not
12 500 pages. It is one page. So it is very basic. It
13 is not at all as technical as, for example, the
14 implementation of the NIST cybersecurity controls that
15 the STAR workgroup, or strategic threat and response
16 workgroup, from the Security Summit is working on.

17 We are not aware of any other global security
18 standard applicable in the tax industry. And, as I
19 just mentioned or as John mentioned, the FTC safeguards
20 rule appears to be focused only on tax return preparers
21 who are focused on individual taxpayers, as opposed to
22 business taxpayers. So we believe that is a gap given

1 where the fraudsters are moving to steal data and
2 breach the tax system.

3 The other thing that John mentioned is the
4 IRS doesn't appear to have enforcement authority under
5 the FTC safeguards rule because the enforcement
6 authority is with the FTC. So we think these gaps need
7 to be clarified and closed.

8 So recommendation 5 is recommending that
9 Congress establish a common security standard and IRS'
10 authority to enforce it. That would be across both
11 individual and business tax returns. We think the
12 extension of the FTC safeguards rule has certain
13 advantages to it because it is a longstanding rule and
14 because it is pretty straightforward, but there may be
15 some other suitable legislation. So we kind of view
16 this recommendation as directional.

17 Recommendation 6 is focused on a related
18 point. The Security Summit's STAR working group is
19 working to implement common security controls within
20 the electronic tax system. And so it is a level of
21 granularity down from the FTC safeguards rule. The
22 STAR workgroup has made significant progress in that

1 area with both its tax and payroll subgroups, but we
2 still think there is an opportunity to increase
3 participation. So recommendation 6 encourages the IRS
4 to increase participation in the STAR workgroup efforts
5 by identifying and removing barriers to participation
6 or increase participation or even potentially finding
7 incentives to encourage increased participation.

8 So I am going to shift now from the
9 recommendations that were focused on establishing
10 common security standards and practices to
11 recommendations focused on increasing the security
12 profile of tax professionals.

13 Tax professionals provide some unique
14 challenges, principally because of their large number.
15 I believe there are on the order of 700,000 preparer
16 tax identification numbers issued annually, and there
17 are some 300,000 electronic return originators which
18 are, in fact, tax professionals or tax professional
19 firms, issued annually. So there are "several hundred
20 thousand," in quotes, tax professionals out there. And
21 so any solution has to be scalable, and it has to be
22 light touch. And we think that there are opportunities

1 here.

2 Now, fortunately, many preparers are part of
3 a larger organization, whether it is a firm or an
4 organization of some type. So they have some support
5 in the area of information or cybersecurity, but not
6 all do. There are many smaller practitioners.

7 So our recommendations in this area are
8 essentially focused on three things: increase
9 awareness, increase understanding, and increase
10 accountability. So how do we increase awareness? IRS
11 has already made a strong effort to communicate with
12 tax professionals. Some of the tax communications
13 campaigns have been mentioned, "Don't Take Tax and
14 Security Together," "Don't Take the Bait," and others.
15 And there is another one coming out, "Security 101" or
16 something along those lines, that is even improving on
17 those campaigns.

18 So as a part of those campaigns, there are a
19 number of different points being made to tax
20 professionals. The one recommendation we have in terms
21 of recommendation number 8 is to emphasize to tax
22 professionals that information security is not just

1 good business. It is the law. Any tax professional
2 serving an individual taxpayer is covered by the FTC
3 safeguards rule. And recommendation number 7 is
4 focused on reinforcing that point that they have a
5 legal obligation.

6 Increasing awareness is not enough. What we
7 also want to do is increase understanding. The IRS
8 does recognize security education as part of the
9 credits that are permitted to qualify or certify
10 certain types of tax professionals. We believe that we
11 should take the available security education
12 opportunity and make it a requirement, that tax
13 professionals should have an education or continuing
14 education requirement of one or two hours a year in the
15 security area in order to drive increased
16 understanding, not just increased awareness. And then
17 we would take that even a step further.

18 Recommendation number 9 is focused on
19 providing more accountability. And one of the ways to
20 provide more accountability is to obtain from tax
21 professionals either some type of an acknowledgement or
22 an attestation that they either understand their legal

1 obligations under the FTC safeguards rule or they are
2 in compliance with the FTC safeguards rule. So the
3 focus of the recommendations is increase awareness,
4 increase understanding, increase accountability.

5 And, then, finally, as we have looked through
6 this area, it appears there are a number of different
7 IRS organizations responsible for setting security
8 requirements and providing security guidance depending
9 on the role that the tax professional or the hat that
10 the tax professional is wearing. Tax professional
11 might be an electronic return originator, or an ERO.
12 They may be a practitioner, a CPA-enrolled agent or
13 attorney covered by the Circ. 230. It may be, he or
14 she may be, an unenrolled preparer. They might even
15 be, like me, a VITA volunteer. Every one of those four
16 hats has a different organization with IRS responsible
17 for it, whether the return preparer organization, the
18 Office of Professional Responsibility, SPEC, Electronic
19 Products and Services. And so what we believe is that
20 having different organizations develop separate
21 security requirements and guidance creates
22 inconsistency and duplication of effort. And we would

1 encourage the IRS to empower one organization within
2 the agency with overall responsibility for setting
3 requirements for tax professionals and then coordinate
4 the implementation of these requirements through those
5 other stakeholder organizations.

6 So that wraps up my area of recommendations.
7 I am going to hand off to Mike Jackman, who will
8 discuss our final set of recommendations.

9 MR. JACKMAN: Good morning. I promise I
10 won't fall again.

11 (Laughter.)

12 MR. JACKMAN: Just a little extra
13 entertainment.

14 My name is Mike Jackman. I just completed my
15 50th year in the taxation field. I am an enrolled
16 agent.

17 (Applause.)

18 MR. JACKMAN: Thank you. Thank you.

19 I am an enrolled agent with a small tax
20 practice. And, like Phil, I am also a VITA volunteer,
21 been involved in electronic filing since the beginning
22 in 1986. So I am going to be presenting the last six

1 recommendations in the area of enabling electronic tax
2 services and increasing electronic filing.

3 First look at the electronic tax services or
4 online tools that the taxpayers and tax practitioners
5 use. The IRS has a long history of experience in this
6 area, going way back to the 1970s. Their first
7 automated tool was the refund status tool, which is now
8 "Where's My Refund?" And, of course, millions and
9 millions of people have used that to find out the
10 status of their tax refund, very successful.

11 In the 1990s, they introduced a suite of
12 professional tools, which included transcripts, powers
13 of attorney, tax return transcripts, many other items.
14 It is a great suite of tools for the tax professionals.

15 In 2014, they released a future state
16 concept, which envisions how the IRS will interact with
17 the public in the future. In 2016, the first future
18 state applications came online: a limited tax account,
19 which is called "How Much Do I Owe?"; online payments;
20 and online payment agreements, all very successful.
21 However, again, I am back to the rest of the theme that
22 you have heard across the board today: security.

1 Security is the foundation for any IRS online service.
2 The IRS must have rock-solid identity proofing and
3 authentication to have successful online services. The
4 next two recommendations focus on those areas.

5 Identity proofing is one of the challenges to
6 the successful spread of online used by taxpayers.
7 Currently the IRS requires a method called Secure
8 Access for taxpayers and practitioners to use many
9 online tools, the ones that have a lot of confidential
10 information contained in them. To get online secure
11 access, a taxpayer or a practitioner must have an email
12 address, a credit history, and a mobile phone that is
13 U.S.-based, and register online successfully with those
14 items.

15 What we have found is a significant
16 percentage of taxpayers are unable to do this. So we
17 looked at ways that maybe this could be expanded to
18 other than an online program that requires those items.
19 We looked at, of course, face-to-face identity
20 proofing, which is the first thing that comes to mind.
21 A person can come into an IRS office, show their
22 identification, and be authenticated and be allowed to

1 have access to the system. Also, if the IRS only has a
2 limited number of taxpayer assistance centers, if they
3 wanted to expand that further, they could maybe partner
4 with another government agency, such as Social Security
5 Administration or other agencies that have offices in a
6 more varied geographic area.

7 However, both of these options are costly,
8 both in terms of labor for the government and for the
9 public in terms of time and travel. So we looked at
10 what some of the other alternatives may be. And we
11 came up with what is called a trusted third party. And
12 that is the area of our first recommendation I am going
13 to discuss.

14 These trusted third parties would be tax
15 professionals or other individuals who have been
16 through the proper vetting and have provided proof of
17 training. This is similar to the certified acceptance
18 agent that is used for issuing ITINs. Certified
19 acceptance agents have gone through a background check,
20 fingerprint check. They have to provide proof of
21 taking certain courses, such as an identification
22 document, forensics course. We recommend that a

1 similar type of vetting be done for the trusted third
2 party for the online secure access. And that is our
3 first recommendation in this group. ETAAC recommends
4 that the IRS investigate this option.

5 The next one in the area of security is the
6 -- I think John mentioned it earlier, the identity
7 theft identification number, the IP PIN. The IP PIN
8 has been used in a number of years now and issued to
9 people who have been identified as victims of identity
10 theft. And how the IP PIN works is on their next tax
11 return, they have to furnish this IP PIN, and it must
12 match the number furnished by the IRS to them for that
13 year.

14 Recently, that was expanded to more than just
15 those people who are victims of identity theft.
16 People, taxpayers, in the States of Florida, Georgia,
17 and the District of Columbia were allowed to request
18 IP PINs. If they wanted one, they could go online and
19 obtain an IP PIN.

20 What we looked at is in the current climate
21 with all of the data breaches that have gone on
22 nationwide in the last few years, every taxpayer is at

1 risk of identity theft and every taxpayer should have
2 the option of opting in and getting an IP PIN so that
3 they can help prevent unauthorized use of their tax
4 data. Taxpayer Advocate has come up with this
5 recommendation, and we recommend and agree with the
6 Taxpayer Advocate that the IRS allow nationwide opt-in.

7 Okay. The next area I want to look at is a
8 little different focus and some stakeholder
9 involvement. In the future state concept that I
10 mentioned before, the IRS is committed to incorporate
11 perspectives from employers, taxpayers, tax
12 professionals, partners, and other stakeholders. We
13 believe that the IRS has taken some of the first steps
14 in meeting this commitment. They have done tax
15 professional surveys. Thirteen hundred tax
16 professionals responded. And, as a result of those
17 responses, the prototypes were demonstrated, were
18 developed and demonstrated, in 2017 tax forms, feedback
19 solicited, and the IRS is using that feedback to
20 further refine their future state.

21 However, we encourage these efforts, and we
22 do believe it can be enhanced two ways: first, by

1 increasing its engagement with stakeholders concerning
2 the features design and implementation of its digital
3 services and the IRS be more transparent about publicly
4 reporting on goals for both customer service metrics,
5 stakeholders' feedback, and other key elements of the
6 digital strategy.

7 Okay. We will move on to the next one:
8 online power of attorney. This is the first of the
9 actual online applications we are talking about
10 recommending. And this would be a secure power of
11 attorney electronic submission. Both the taxpayer
12 representative and the taxpayer would have to
13 authenticate to the secure access, the system that I
14 mentioned before. And the taxpayer through that secure
15 access system would be giving the representation to
16 that tax professionals. There would be minimum
17 standards imposed upon anybody participating in this
18 tax professional-wise. They would have to be either,
19 we recommend, Circular 230 participant or be involved
20 in an IRS-sponsored program, such as VITA. This would
21 allow for a seamless online experience via the tax
22 professional account in solving identity theft and

1 other tax issues without delay. We recommend that IRS
2 implement online power of attorney as a priority.

3 The final recommendation I am going to speak
4 about is relating to increasing electronic filing. It
5 is the e-filing of employment tax returns. As John
6 mentioned earlier, 94X returns represent the second
7 highest number of returns filed. While 40 million
8 returns filed a year, many of them are the quarterly
9 withholding and Social Security returns as well as the
10 annual unemployment tax, computer tax returns. And
11 there is also an annual employment tax return, 40
12 million of them filed each year. Only about 30 percent
13 of that 40 million are filed electronically, about 12
14 million. The most commonly cited areas among
15 particularly the small- and medium-sized either
16 employer or tax professional because many of these are
17 filed directly by employers is that the IRS requires a
18 third party software and transmitter to file
19 electronically these types of returns. And there is a
20 multi-step registration process that each 94X client
21 must complete.

22 Increasing the number of 94X returns would

1 assist in exceeding the goal of the 80 percent of all
2 major returns filed electronically. We recommend that
3 the IRS leverage its public-private partnerships to
4 establish a collaborative undertaking with all key
5 stakeholders using a 2-phased approach for 94X returns.
6 First is focusing on improving IRS communications. And
7 the second is focus on streamlining IRS policies and
8 procedures.

9 With that, I thank you. This concludes our
10 recommendations for 2018. And I turn it back to John
11 Sapp.

12 CHAIR SAPP: Thank you, Mike. Everybody is
13 watching.

14 (Laughter.)

15 CHAIR SAPP: At this time, I would like to
16 open up the panel for any comments from the IRS.
17 Terry, I will start with you.

18 MR. LEMONS: Sure. First of all, let me hand
19 it over to Mike Beebe, who is the director of our RICS
20 organization, which is kind of frontline in the whole
21 battle against fraud as well as identity theft. In
22 addition to running RICS, Mike is the point person

1 right now for the IRS side of the Security Summit
2 effort. And, like the other team leads we have up here
3 on the podium as well as some key players here in the
4 room on the IRS side, the Security Summit work is in
5 addition to their regular duties. So let me hand it
6 over to Mike.

7 MR. BEEBE: All right. Thank you, Terry.

8 I just want to take the opportunity to thank
9 the ETAAC and all of its Committee members. I
10 certainly appreciate your dedication and commitment to
11 protecting the American taxpayer. I definitely want to
12 thank John Sapp for your leadership over the last two
13 years. So thank you very much. We will certainly miss
14 you in that role but glad to have Doreen and Phil in
15 their new roles and welcome them and look forward to
16 working with them as a part of the Security Summit,
17 also look forward to working with our state and
18 industry Security Summit partners to address the ETAAC
19 recommendations. I will say that some progress has
20 already been made on some of the areas, such as
21 expanding membership to the summit as well as to the
22 ISAC, increased communications, and providing enhanced

1 protections against business identity theft. Some of
2 the recommendations will be a little bit more
3 challenging; in particular, around IP PIN, expanding
4 that, and implementing a lock and unlock due to budget
5 and IT restraints. However, we do continue to pursue
6 those efforts.

7 Again, thank you. And I would like to turn
8 it over to Edwards Killen. Edward is the director of
9 PGLD, and he is the lead for the Security Summit
10 information-sharing working group. Edward?

11 MR. KILLEN: Thanks, Mike.

12 I would echo the sentiments expressed
13 throughout the day here of appreciation to the ETAAC
14 membership on your very thoughtful recommendations and
15 the work that you have put in. I think it is
16 exemplary, and it is an example of the power of public-
17 private partnerships when you bring thoughtful, well-
18 meaning people together to resolve an issue that none
19 of us can resolve effectively individually, but
20 collectively we are much stronger. So I would like to
21 thank you for just the dedication, not just this year
22 but over the past few years.

1 Also, I would be remiss if I didn't publicly
2 thank Mike for the leadership that he has exhibited
3 within IRS. You know, IRS is a large organization.
4 And it can be very difficult wrangling all of us
5 together to do the good work of all of the various
6 working groups that we have. And also I would like to
7 thank Todd for his leadership in standing up the ISAC.
8 You know, the Security Summit has been an example of
9 both the benefit and the difficulty oftentimes of doing
10 something that hasn't been done before. And you can
11 only accomplish that if you have great leadership. And
12 so both of these folks have exhibited great leadership
13 in that regard. Again, the recommendations are
14 thoughtful, and it is very clear the level of due
15 diligence that you all undertook over the course of the
16 past year in coming up with these.

17 One thing that I do want to mention because I
18 think Mike alluded to the fact that we have begun a lot
19 of work that addresses some of the recommendations that
20 you have -- and as I sort of listened earlier, I was
21 reminded of, you know, the Security Summit criteria.
22 And the membership process I think have been very good

1 because I think what it speaks to -- and I have heard
2 Mike talk about this -- is the need for us to
3 operationalize the work that we have done in the
4 Security Summit and ISAC. So, you know, this is really
5 our fourth year of working together, but we have had
6 sort of three full seasons. And I think we have a
7 shared interest in ensuring that this is a process that
8 exists outside of the power of individual personalities
9 that may be working at any given time but really set
10 this partnership up and this collaboration up in a way
11 that is sustainable. And I think having solid
12 membership criteria and expectations and a process to
13 expand outreach and bring new members in who can add
14 value to our collective work, I think that is extremely
15 important. And, you know, the recommendations, I think
16 the consistent theme here around membership expansion,
17 around looking for new tools, innovation due to work
18 that we are doing and around just the overall
19 importance of security, I think that is extremely
20 important because to the extent that we are all one
21 chain, we are only as strong as the weakest link in
22 that chain. And so I think the work that you have done

1 to really sort of elevate all of the members of the
2 ecosystem I think will do nothing but benefit tax
3 administration and our taxpayers. At the end of the
4 day, that is really what we are all trying to do. So
5 thank you for the work.

6 MR. EGAAS: Yes. I would echo the comments
7 about thank you, ETAAC, in your wise guidance and your
8 recommendations. And, you know, the ISAC wouldn't be
9 here if it weren't for my colleagues, you know, in the
10 room and up here on the stage but also the industry
11 members and the state members that came together to put
12 all of this together. And there are several ETAAC
13 members who also serve on the senior executive board of
14 the ISAC. And so as we look to put in place the
15 recommendations that ETAAC has brought forth, you know,
16 I will seek their counsel on how we make this work.

17 An implicit goal of the ISAC I think is to
18 kind of raise everyone up. There is a wide spectrum of
19 capabilities across industry and states. And so, you
20 know, as we look to continue what we are doing with the
21 ISAC being a special place of collaboration, I think
22 that is always something in the back of my mind that if

1 we can educate and help people, you know, fight this
2 fraud together, we will all be in a much better place.
3 So thanks, all, for your efforts.

4 MR. LEMONS: All right. And just to kind of
5 wrap up a little bit, you know, put my summit
6 communications hat on here. You know, one thing I just
7 think looking at the communications effort, I think
8 there is some really good information here in the
9 report. And, you know, I thank John and the team for
10 taking a look at it.

11 We have made I think a lot of progress on the
12 communications front as far as education over the last
13 couple of years. And it has been a real collaborative
14 effort. You know, especially over the last year, I
15 think we have made some real progress working jointly
16 with the states, with the national tax associations,
17 with the financial industry, you know, the payroll
18 community. I mean, it has really been a very multi-
19 pronged effort. And I really think we are making some
20 difference.

21 We have had a lot of support inside the IRS
22 as well, from Wage and Investment, Criminal

1 Investigation, PGLD, Return Preparer Office, really,
2 you know, as well as my team in NPL and my other
3 functions helping support that.

4 But I think, even with all of that, I mean,
5 it is very clear from your report that, you know, we
6 need to do more. I was busy furiously taking notes on
7 a couple of your recommendations.

8 And, as Phil noted in his comments, we are
9 gearing up for another awareness effort this summer
10 that will be focused on tax professionals. Basically,
11 it is going to be called Tax Security 101. It will be
12 starting in July. And we will be doing a series of
13 news releases there. We are also pairing it up with
14 the nationwide tax forums, which will be starting July
15 10th in Atlanta. And, you know, there were a couple of
16 references in the report.

17 We are also trying to take up, you know,
18 increase our efforts at the forums to add some
19 additional voices to discuss the whole security angle.
20 And I know the summit effort and after helped support
21 bringing in an outside group to help us with that
22 effort this summer. So I appreciate that.

1 But basically we are going to keep on
2 plugging away at this. And, you know, I think there is
3 more we can do. And we really appreciate the ETAAC
4 support on, you know, looking at the communications and
5 giving us, you know, a clear view in terms of some next
6 steps. It has been very helpful for me in that role
7 having that, having the guidance and insight.

8 So I think anybody else on the IRS side have
9 any comments? I know we have got several key players
10 here in the room not at the podium.

11 CHAIR SAPP: We do have a microphone.

12 (No response.)

13 MR. LEMONS: Okay. I think that is it for
14 the IRS.

15 CHAIR SAPP: Well, that brings us to the end
16 of our meeting. We are ahead of schedule. I will just
17 point that out as a bar for Doreen in the future to
18 shoot for.

19 As we close, I think I would be remiss if I
20 didn't just point out a couple of things. My
21 background is as a CPA. I have been in tax not as long
22 as Mike, of course, but since the mid '80s.

1 Historically, tax professionals and, by implication,
2 tax software companies have had an antagonistic I would
3 say relationship with the IRS. And we have always
4 looked at them historically as a necessary evil.
5 Whenever we were advocating for our clients as
6 taxpayers, it appeared as if there was roadblock after
7 roadblock almost any time you needed to deal with the
8 IRS. The IRS we have learned would look with some
9 doubt on the integrity of some tax professionals as
10 they dealt with the Internal Revenue Service. And
11 state departments of revenue, I won't go even down that
12 path of how bad those relationships could be at
13 different times depending on the issue.

14 One thing the Security Summit has done and if
15 there is a benefit to the problem of ID theft and
16 refund fraud is we have each seen issues that impact
17 our greater public and our republic. We have seen
18 those issues from multiple perspectives. ETAAC
19 represents that, but the Security Summit on a weekly
20 basis, those conversations occur. We now see the IRS'
21 true desire to serve taxpayers. I can remember rolling
22 my eyes when that initiative first came out that the

1 IRS was going to be a customer service organization.
2 But seeing the commitment, starting with the
3 executives, many at this table, many sitting in the
4 audience, and permeating throughout that organization
5 over the last four or five years during the Security
6 Summit, I think each of us has been amazed at the
7 dedication not only for administering the tax system
8 and serving multiple stakeholders within Washington,
9 D.C. and the Beltway but their commitment to helping
10 taxpayers meet their tax obligations but also truly
11 become what I consider to be for the size of the
12 populous that they serve and the budget that they have
13 a very customer-centric service organization to help
14 taxpayers.

15 It has been an education for me personally to
16 see that level of commitment and the level of
17 professionalism for the teams involved with the
18 Internal Revenue Service. They are an incredible
19 organization and one that we are privileged to work
20 with.

21 The biggest thing that has occurred over the
22 last four years in my estimation within the stakeholder

1 groups is trust. I can tell you there is a high level
2 of trust now between an industry that historically has
3 not leaned toward trust as a strong suit and the
4 Internal Revenue Service and state departments of
5 revenue and tax professionals all the way down the
6 line. There is a high level of trust now that everyone
7 is motivated to solve this problem: ID theft, tax
8 refund fraud, secure access to systems, and helping
9 taxpayers meet their obligations and receive their
10 refunds in a timely fashion. So I don't know a better
11 way to say that. I wish I could articulate that
12 better, but the level of professionalism within the
13 groups involved in the security summit is extremely
14 impressive. And we as a country are fortunate to have
15 that level of expertise, I believe.

16 So, with that, I will bring us to a close and
17 just say thank you for coming today. I encourage you
18 to grab a hard copy of our report. Take it home. Read
19 it to your children --

20 (Laughter.)

21 CHAIR SAPP: -- especially if they are small
22 and it is time to go to bed.

1 (Laughter.)

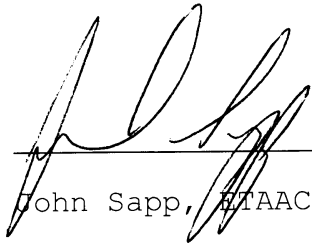
2 CHAIR SAPP: So thank you for your time, and
3 thank you to our ETAAC Committee and the IRS.

4 (Applause.)

5 (Whereupon, at 10:54 a.m., the meeting was
6 adjourned.)

7

8

9 Approved:  _____
10 John Sapp, ETAAC Chair

Date: 9/18/15

11

12

13

14

15

16

17

18

19

20

21

22

1

2