2011

Tax Data Security

ETAAC Software Subcommittee

Recommendations to ETAAC

This document summarizes key recommendations of ETAAC Software Subcommittee Security Working Group. The full description of our recommendations is contained in a final written report, which should be considered the authoritative description of our recommendations. As a result, this summary should not be quoted by third parties.

Phil Poirier, VP-Gov't, Intuit Consumer Group

Dave Olsen, CPA, Dir–Product Mgmt, CCH Small Firm Services

Timur Taluy, CEO, Fileyourtaxes.com

2011

Internal Revenue Service SDC Software Developers Conference

Objective: Report…Discuss

Report the security recommendations from the ETAAC Software Subcommittee Security Working Group (WG)

- **Today's review will cover…**

–WG's investigation and research

  - Reported at ETAAC December '10 Public Meeting

–WG's recommendations to ETAAC

  - Reported at ETAAC March '11 Public Meeting

- **Panel – State of the Industry**

2011

Internal Revenue Service SDC Software Developers Conference

News no one wants to hear…

"In a CDW report on threat prevention, *data loss* emerged as the No. 1 cybersecurity challenge faced by… businesses… "

2011

Internal Revenue Service SDC Software Developers Conference

News no one wants to hear…

"The Massachusetts Executive Office of Labor and Workforce Development has admitted belatedly that personal information on up to 210,000 unemployed residents may have been compromised as the result of a cyber-attack…"

2011

Internal Revenue Service SDC Software Developers Conference

News no one wants to hear…

"The Department of Health and Human Services (HHS), which has been doling out millions in fines for failing to protect the privacy of patient information, has been found wanting in that area by the department's Office of the Inspector General (OIG)…"

2011

Internal Revenue Service SDC Software Developers Conference

News no one wants to hear…

"In response to recent data breaches at RSA, Epsilon, and Sony, a group of five Democratic senators is asking the Securities and Exchange Commission (SEC) to issue national guidelines regarding breach disclosure…"

2011

Internal Revenue Service SDC Software Developers Conference

What if…

"In other news, the IRS has acknowledged personal data on 73 million taxpayers held by e-file transmitters has been compromised…"

First Steps…

Investigation & Research

2011

IRS forms ETAAC Software Subcommittee

2009 GAO Report

- Industry files 100% of e-filed individual returns

- IRS needs to understand the risks

IRS Electronic Tax Administration Advisory Committee (ETAAC)

Reps from:
IRS
States
Industry
ETAAC

ETAAC Software Subcommittee

Formed late 2009

Security & Privacy Working Group

Accuracy & Reliability Working Group

2011

Recommendations Process

3 **IRS**

IRS will make its own decisions, as it does with any recommendations

Report to Congress (June '11)

2 **IRS Electronic Tax Administration Advisory Committee**

Currently considering Subcommittee's recommendations

*** Recommendations (March '11)**

1 **ETAAC Software Subcommittee**

Conducted investigation and review between Dec '09 / Mar '11

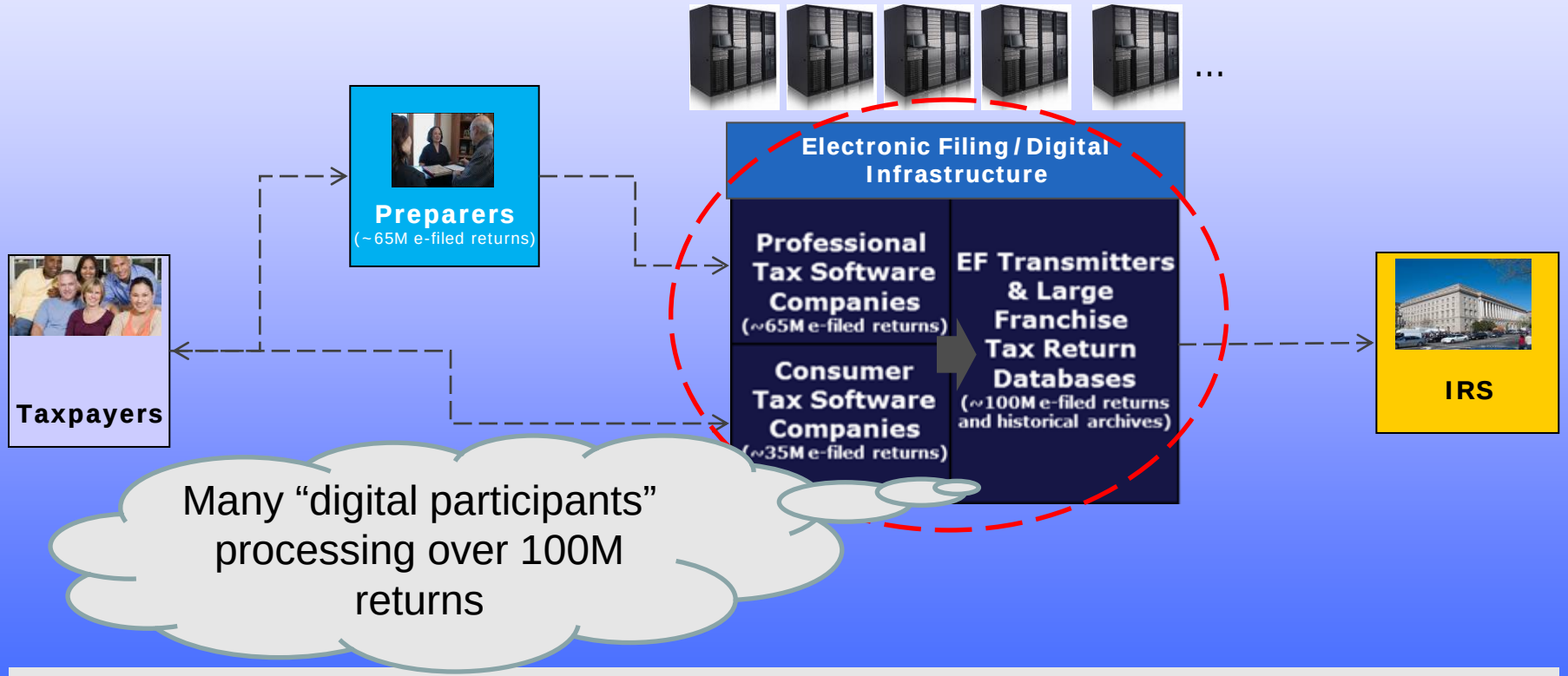
* Subcommittee's ETAAC Public Meeting presentations accessible in GSA's "FACA Database"

2011

Internal Revenue Service SDC Software Developers Conference

Working Group initial focus: e-file "digital infrastructure"

Highest risk area given high volume of electronic returns, but industry diversification helps to mitigate risks



These Recommendations do not cover preparers/EROs -- ETAAC will likely consider other such areas in the future

2011

Internal Revenue Service SDC Software Developers Conference

E-file Provider Information Security Program Already Required

- **FTC Safeguards Rule provides a high level outline for a *comprehensive information security program***
  - ✓ Designate staff
  - ✓ Conduct risk assessments
  - ✓ Conduct safeguards assessments -- *assessing sufficiency of safeguards to control risks, including employee training and management, IT systems security, and detecting/preventing/responding to attacks and intrusions*
  - ✓ Implement, test and monitor safeguards -- *designing and implementing information safeguards and regularly test and monitor effectiveness*
  - ✓ Oversee third parties – *engaging service providers that are capable of maintaining appropriate safeguards for the customer information*
  - ✓ Adjust the program as the environment changes -- *evaluating and adjusting information security program based on testing and monitoring, changes in operations, and other circumstances*

2011

Internal Revenue Service SDC Software Developers Conference

IRS asked Subcommittee: Recommend in 4 key areas

1. **Standards**: What additional guidance or standards should IRS set in connection with the current responsibility of Authorized IRS e-file Providers to comply with the FTC Safeguards Rule?

2. **Review**: What review methodology should IRS require to ensure that Providers are complying with the FTC Safeguards Rule and any other relevant security standards?

3. **Validation**: What approach should IRS take to ensure that it is informed whether a particular company has successfully completed any security review and is meeting applicable standards?

4. **Implementation**: What plan/schedule should IRS follow to implement any new security requirements in this area?

Not a question of whether there should be security requirements…a question of how to enhance existing compliance

2011 Internal Revenue Service SDC Software Developers Conference

Working Group used a rigorous, deliberative approach

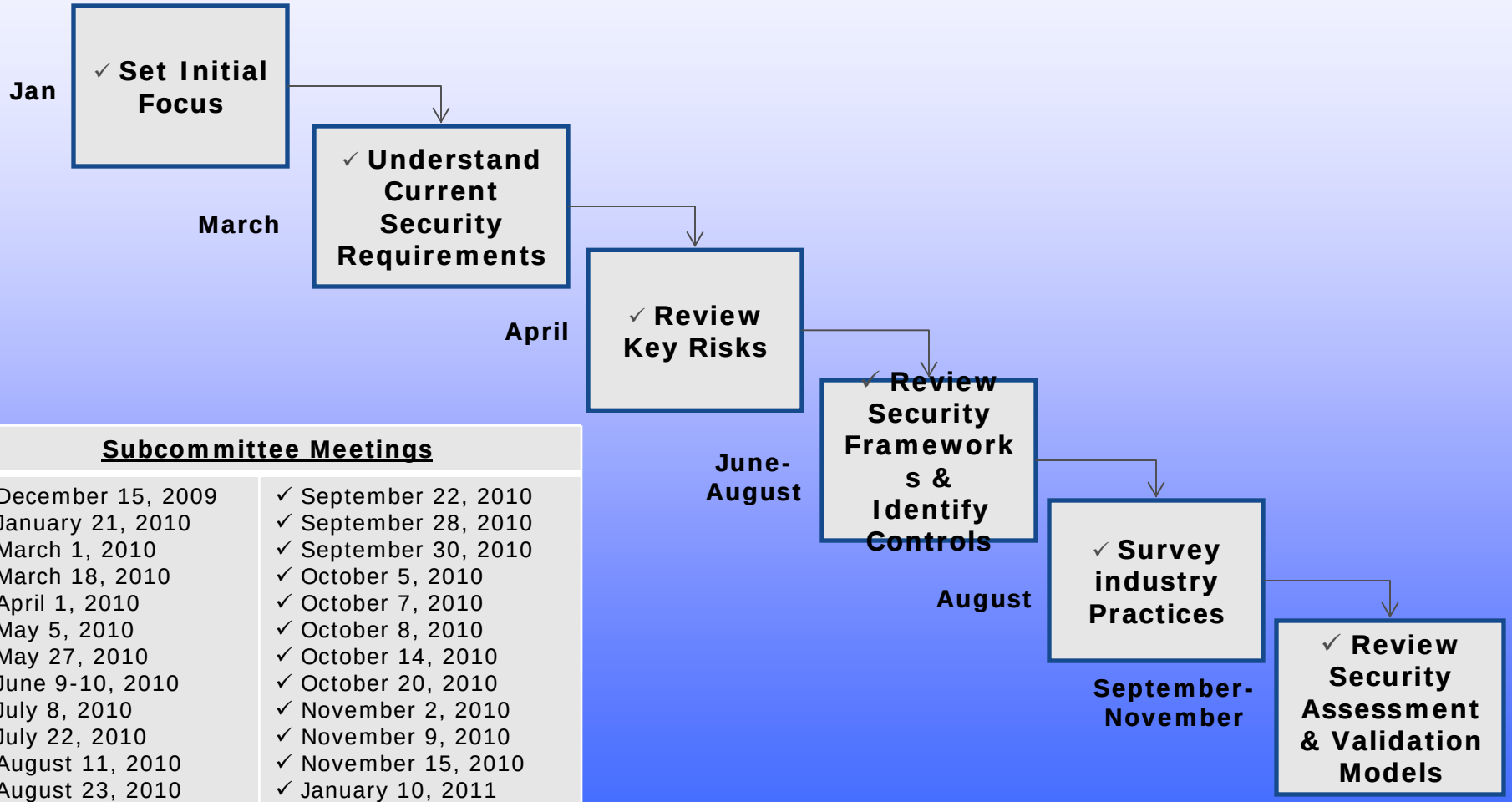
Information considered by the Working Group…

- IRS e-file Provider security requirements
- Reports on security threats, risks, and implications
- Security frameworks/requirements (with outside experts)
- Qualitative feedback from industry on current security practices
- A broad array of industry and government security assessment models
- FTC Safeguards Rule enforcement actions (with FTC staff)

2011

Internal Revenue Service SDC Software Developers Conference

Significant time committed…
> 25 meetings & 1,000+ hours



Subcommittee Meetings

- ✓ December 15, 2009
- ✓ January 21, 2010
- ✓ March 1, 2010
- ✓ March 18, 2010
- ✓ April 1, 2010
- ✓ May 5, 2010
- ✓ May 27, 2010
- ✓ June 9-10, 2010
- ✓ July 8, 2010
- ✓ July 22, 2010
- ✓ August 11, 2010
- ✓ August 23, 2010
- ✓ September 16, 2010
- ✓ September 22, 2010
- ✓ September 28, 2010
- ✓ September 30, 2010
- ✓ October 5, 2010
- ✓ October 7, 2010
- ✓ October 8, 2010
- ✓ October 14, 2010
- ✓ October 20, 2010
- ✓ November 2, 2010
- ✓ November 9, 2010
- ✓ November 15, 2010
- ✓ January 10, 2011
- ✓ February 23, 2011

Next Steps…

Conclusions & Recommendations

2011

Internal Revenue Service SDC Software Developers Conference

Conclusions Driving Recommendations

- Attractive Data Target
- Breaches Affect Confidence
- Safeguards Rule Provides High Level Framework
- IRS should Supplement Self Interest
- Controls + Assessments = Reasonable Assurance
- Balance Benefit / Burden
- Seasonality and Deadline Factors
- Start with Education & Collaboration

2011

Internal Revenue Service SDC Software Developers Conference

IRS's critical role in a *living process*

2011

Internal Revenue Service SDC Software Developers Conference

Recommendations: *Scope*

- **Who** - IRS E-File Program Digital Infrastructure Participants
  - Transmitters, Software Developers, Online Providers & Intermediate Service Providers
- **What** - Taxpayer accounts and personal information
  - Initial phase relates to individual and business income tax returns.
  - Deferred employment returns (94X series) and information returns for later consideration
- **Where** - Taxpayer Data Environment
  - Network components, servers, applications or IT assets
  - Related organizational, physical environment and process components

Recommendations: *Standards*

- **Require implementation of selected NIST SP 800-53 controls**
  - Balance of flexibility and specificity that industry needs
  - NIST 800-53 controls selected based on their contributions to enhancing information security and their relevance to industry

2011

Internal Revenue Service SDC Software Developers Conference

Recommendations: *Assessments*

Accountability	Company senior management is accountable for implementing a comprehensive information security program
Certification / Reasonable Assurance	Senior management should annually certify the company had reasonable assurance of the security, confidentiality, and integrity of personal information
Assessment Cycle	Annual *self assessment* by internal security staff Triennial *third party assessment* by independent external experts
Reporting	Companies report results of assessments to IRS

2011 Internal Revenue Service SDC Software Developers Conference

Recommendations: *IRS Validation*

- **IRS "spot checks" performance and practices**
  - Risk-based
  - Random selection
  - Event-driven
- **Deficient spot check results should have consequences**
  - Increased frequency for third party assessments
  - Suspension of company from the e-file program or other IRS enforcement actions
  - Prohibition on assessors being used for third party assessments

2011

Internal Revenue Service SDC Software Developers Conference

Recommendations: *Implementation Phase-in*

Companies <u>immediately</u> begin providing self-assessment certifications

PROGRAM LAUNCH
- ✓ Program Development
- ✓ Initial outreach
- ✓ Program launch
- ✓ FTC Safeguards <u>self-certification</u>

END OF "YEAR 1" 1
- ✓ Ongoing outreach
- ✓ NIST Priority 1 Controls implementation completed
- ✓ FTC Safeguards <u>self-certification</u> inc'l NIST Priority 1 Controls

END OF "YEAR 2" 2
- ✓ Ongoing outreach
- ✓ NIST Priority 2 Controls implementation completed
- ✓ FTC Safeguards <u>self-certification</u> inc'l NIST Priority 1 & 2 Controls

FULL IMPLEMENTATION

END OF "YEAR 3" 3
- ✓ Ongoing outreach
- ✓ NIST Priority 3 Controls implementation completed
- ✓ FTC Safeguards <u>third party</u> certification inc'l NIST Priority 1,2&3 controls

Implementation Details: *Assessor Qualifications*

Self-assessor qualifications

- *College Degree*
- *Company IT Systems Experience* – minimum 3 years
- *Security IT Experience* – minimum 3 years

Third party assessor qualifications

- *Active Business Requirement*
- *Professional & Ethical Standards*
- *Certification & Experience Requirements*
  - Security certifications such as: CISSP, CISA, CISM, GSEC, GISP or QSA, and
  - At least 5 years experience

Implementation Details: *Controls Phase-in*

Recommend phasing in selected NIST 800-53 controls over a 2-3 year period in the following prioritized order:

Priority 1 Controls (first 12 months):

AC, AT, IA, IR, PE, PS, SC & SI

- AC: Access Control
- AT: Awareness and Training
- IA: Identification and Authentication
- IR: Incident Response
- PE: Physical and Environmental Protection
- PS: Personnel Security
- SC: System and Communications Protection
- SI: System and Information Integrity

2011

Internal Revenue Service SDC Software Developers Conference

Implementation Details: *Controls Phase-in*

Recommend phasing in selected NIST 800-53 controls over a 2-3 year period in the following prioritized order:

Priority 2 Controls (following 12 months): AU, CA, CM, MP, PM, RA

- AU: Audit and Accountability
- CA: Certification, Accreditation, and Security Assessments
- CM: Configuration Management
- MP: Media Protection
- PM: Program Management
- RA: Risk Assessment

Priority 3 Controls (following 6 months): MA, SA

- MA: Maintenance
- SA: System and Services Acquisition

State of the Industry

- Follow up comments
- Questions