



FTA E-file Symposium
May 20-23, 2007

Where Are the Security Guidelines for Protecting Taxpayer Data?

Carolyn E. Davis,
Sr. Program Analyst/Project Manager
Internal Revenue Service
Carolyn.e.davis@irs.gov

1



FTA E-file Symposium
May 20-23, 2007

Agenda

- Background
- Progress Update
- Next Steps
- Questions

2



FTA E-file Symposium
May 20-23, 2007

ETA Security Summit

Electronic Tax Administration

- **Hosted** e-file Security Summit with industry, states, IRS stakeholders in November 2004
- **Formed** Committee on Standards and Protecting Taxpayer Electronic Data (SSPTED)
 - Internal and external partners
 - Researched existing laws
 - Met with FTC to learn about the GLBA

3



FTA E-file Symposium
May 20-23, 2007

TP Involvement

- Obtained trading partner input relating to:
 - development and implementation of standards
 - included approach, challenges, risks, issues, etc.
- Questions we asked:
 - What do you believe are important elements/features that are needed for a standard that ensures taxpayer data security, and are realistic and enforceable?
 - How do you think you can better help your clients in safeguarding taxpayer data?
 - How can IRS assist in this process?

4



FTA E-file Symposium
May 20-23, 2007

Developed the Guidelines

- **Reviewed** current relevant commercial and legal sources
- **Determined** minimum taxpayer data security requirements
- **Requested** Chevo to conduct IRS internal and external stakeholder interviews to understand current practices and requirements
- **Determined** didn't need to re-invent standards
- **Developed** set of guidelines that:
 - Provide the necessary safeguards to taxpayer data
 - Addresses key areas for required safeguards
 - Is scalable and considers the constraints under which Tax Professionals must conduct business
- **Obtained** feedback on drafts

5



FTA E-file Symposium
May 20-23, 2007

Checklists

- The Guidelines include information relating to the following NIST controls:
 - Management
 - Technical
 - Operational
- Presented as easy-to-read checklists:
 - Administrative Activities
 - Facilities Security
 - Personnel Security
 - Information Systems Security
 - Computer Systems
 - Media
 - Certifying Information Systems for Use

6



FTA E-file Symposium
May 20-23, 2007

Educated Stakeholders

ETA

- **Vetted** guidelines with CERCA, FTA TAG, FTC
- **Presented** seminars at IRS Tax Forums (05,06,07)
- **Revised** guidelines – several versions
- **Published** guidelines

7



FTA E-file Symposium
May 20-23, 2007

Published Guidelines

- The guidelines are available on irs.gov:
 - *Safeguarding Taxpayer Data, A Guide for Your Business*, Pub. 4557
 - “*Safeguarding Taxpayer Information, Quick Reference Guide for Business*”, Publication 4600
- Based on:
 - FTC documentation
 - NIST publication 800-53A, *Recommended Security Controls for Federal Information Systems*
- Specifies the *minimum* controls for safeguarding taxpayer data

8



FTA E-file Symposium
May 20-23, 2007

Background – Legal Environment

- **Trading Partners are subject to rules and regulations dealing with protecting the security of taxpayer data from several sources:**
 - **Gramm Leach Bliley Act (GLBA) of 1999** – aka Financial Modernization Act
 - **FTC Privacy of Consumer Financial Information Rule (2001)**
 - **FTC Safeguards Rule (2003)**
 - IRS Revenue Code and Procedures
 - **IRS 6713** – Monetary Penalties for unauthorized disclosure or use of returns and return information by any person engaged in the business of preparing or providing services in connection with the preparation of tax returns
 - **IRC 7216** – Criminal penalties for Disclosure and use of information by any person engaged in the business of preparing or providing services in connection with the preparation of tax returns
 - **Revenue Procedure (latest version)** – Requires *e-file* Providers to abide by GLBA, FTC Privacy and Safeguard Rules, IRC 6713, IRC 7216, and specify penalties for violations
 - **Sarbanes Oxley Act** – Requires covered companies to have controls in place to protect data and disclose information to investors about their investments
 - **State and local laws**

9



FTA E-file Symposium
May 20-23, 2007

New Federal Laws Proposed

- **S.239 – Notification of Risk to Personal Data Act of 2007**
 - A bill to require Federal agencies, and persons engaged in interstate commerce, in possession of data containing sensitive personally identifiable information, to disclose any breach of such information
- **S.495 – Personal Data Privacy and Security Act of 2007**
 - A bill to prevent and mitigate identity theft, to ensure privacy, to provide notice of security breaches, and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information

10



FTA E-file Symposium
May 20-23, 2007

Sources of Further Information

Laws/Rules and Regulations

- Gramm Leach Bliley Act Information - <http://www.ftc.gov/privacy/privacyinitiatives/glbact.html>
- FTC Privacy and Safeguards Rules - <http://www.ftc.gov/privacy/index.html>
- IRC 7216 & 7316
- Revenue Procedure on *IRS e-file*

Security Standards and Guidance

- National Institute of Standards and Technology - Security Standards Documents
- SANS Institute (Sample Security Plans and Policies) – www.sans.org
- Center for Internet Security - www.cisecurity.org

11



FTA E-file Symposium
May 20-23, 2007

Next Steps

- Incorporate comments and suggestions
 - Continue to obtain additional internal IRS input and comments
 - Obtain further input from discussions with trading partners
 - Continue to refine the Guidelines based on input and law changes
- Send comments to:
Safeguard.data.tp@irs.gov

12