



Open Forum Discussion

FTA/IRS Computer Security Conference
April 3, 2008
St Louis

1



Agenda

- Contractor Issues
- Plan of Action & Milestones (POAM) Monitoring
- Incident Reporting

2



Contractor Issues

- Applicable To Which Contracts?
- Contract Language
- 45-day Notification

3



Applicable to Which Contracts?

- Any contractor or subcontractor with potential access to FTI
- Contractor may not be procured through tax agency – may be a broad state contract
- Includes both physical and IT access to FTI

4



Contract Language

- Publication 1075
 - Section 5.4 (page 17)
 - Section 11.3 (page 41)
 - Exhibit 7 (page 77)


5



45-day Notification

- Required by Treasury Regulation
- Submit documentation via SafeguardReports@IRS.gov
- Information to include in notification
 - Type of service covered by contract and duration of contract
 - Contractor name and POC
 - Procedures for agency oversight on contractor access, storage & destruction of FTI


6



Plan of Action & Monitoring (POAM)

- Corrective Action Identification
- Weakness Prioritization & Timeframes
- Monitoring & Reporting
- General Q&A

7



Corrective Action Identification

- Begins in Interim Safeguard Review Report (SRR)
- Agency response to SRR may address identified weakness
- IRS monitoring initiated from Final SRR
- All corrective actions are input into POAM Tool for monitoring

8



Weakness Prioritization & Timeframes

- Severe or catastrophic adverse impact
 - Cause a severe degradation in the loss of IRS mission capability
 - Cause major harm to the IRS's reputation
 - Result in major financial loss to federal taxpayers
 - Agency plan to address weakness must be part of their response to Interim SRR
 - Weakness must be corrected no later than 30 days from date of Final SRR

9



Weakness Prioritization & Timeframes (continued)

- Serious adverse impact
 - Cause a significant degradation in the loss of IRS mission capability – able to perform primary functions but the effectiveness of functions is significantly reduced
 - Cause significant harm to the IRS's reputation
 - Result in significant financial loss to federal taxpayers
 - Agency plan to address weakness must be part of agency response to Interim SRR
 - Weakness must be corrected within 3 months from date of Final SRR

10



Weakness Prioritization & Timeframes (continued)

- Limited adverse impact
 - Cause a significant degradation in the loss of IRS mission capability – able to perform primary functions but the effectiveness of functions is noticeably reduced
 - Cause minor harm to the IRS's reputation
 - Result in minor financial loss to federal taxpayers
 - Agency plan to address weakness must be part of agency response to Interim SRR
 - Weakness must be corrected within 6 months from date of Final SRR

11



Weakness Prioritization & Timeframes (continued)

- Exploited adverse impact
 - Does not have an immediate impact on the confidentiality and integrity of FTI data
 - Warrants corrective action
 - Agency plan to address weakness must be part of agency response to Interim SRR
 - Weakness must be corrected within 12 months from date of Final SRR

12



Monitoring & Reporting

- Agency reporting on corrective actions
 - Use agency response to Interim SRR for all items addressed between the on-site review and receipt of Interim SRR
 - Provide status update on each outstanding corrective action as part of annual Safeguard Activity Report
 - Email status – especially corrective action closures – to SafeguardReports@IRS.gov and Safeguards will close on POAM tool

13



Monitoring & Reporting

- Safeguards will monitor corrective actions
 - Proactive follow up on “severe” and “serious” corrective actions
 - Reconciliation between POAM and agency status updates (SAR/email)
 - Agency follow up if corrective actions not addressed by subsequent SAR

14



Monitoring & Reporting

- Analyzing POAM data on corrective actions
 - Trends by agency type (state tax, child support, welfare or federal)
 - Trends by corrective action category
 - Use identified trends
 - Clarification of Publication 1075 requirements
 - Develop “helpful hints” to post on IRS.gov
 - Targeted outreach


15



Incident Reporting

- New Pub 1075 includes breaches and security incidents in Section 10 requirements
- Contact TIGTA as soon as identify breach that **MAY** involve FTI – don’t wait until investigation complete
- Working with internal functions to identify potential secondary reporting requirement
- IRS required to notify impacted TP in certain circumstances

16



Questions or Other Topics?

17