



Safeguarding Federal Tax Information in a Consolidated Data Center Environment

Janet Miner

Office of Safeguards
Internal Revenue Service

June 8, 2010

Safeguard Program Overview

Safeguards ensures that the federal tax information provided outside the Service is protected as if in IRS hands.

- Oversight of 270 federal and state agencies
- 4.8 Billion tax records disclosed to state tax authorities in 2009
- Goal is to assist agencies in meeting their statutory obligation to protect taxpayer confidentiality for federal tax information (FTI)
- Conduct on site reviews and analyze reports to evaluate security posture. Reviews identify corrective actions. Closing corrective actions is an FY11 priority
- Provide guidance and assistance, phone forums, report prep
- Publication 1075 revision is coming soon
- Incident management for external agency data breaches (loss, theft or misuse)
- Hiring initiative will increase staffing by 1/3, improve service
- Impact of health care legislation TBD

Consolidated Data Centers – Common Issues

- Lack of written agreements related to safeguarding federal tax information
- Statutory limitations on data access is not enforced
- Significant change requires a revised Safeguard Procedures Report
- Use of contractors/subs requires 45-day advance notice to IRS
- Roles and responsibilities for data protection is not clear
 - Authorized agency is the data owner and legally responsible for safeguarding
- Loss of control over the IRS data
 - Where is it? Who can access? Are employees trained?
 - Lack of computer security policies and procedures – enterprise level and/or agency specific to include FTI
 - On site inspection every 18 months, and subject to IRS review; taking corrective action
- Reporting incidents - loss, theft and unauthorized disclosures

Key Points

When IT Operations are consolidated, the authorized agency is responsible for ensuring safeguard standards are met as if it were retained in house

- A new SPR is required
- Computer security policies and procedures updated
- Restricted access must be maintained – no cross-agency access
- 45 day notification of disclosure to contractors
- Training and awareness – annual certification statements
- Service Level Agreements (SLA)
- Reporting data breach incidents

Service Level Agreements (SLA)

Service level agreement, at a minimum, should cover:

- Compliance with Publication 1075 requirements
- Publication 1075, Exhibit 7 language
- Disclosure awareness training requirements
- Internal inspection requirements
- Penalties for unauthorized access or disclosure
- Data breach incident reporting

Outsourcing Information System Management & Support

Key Issues

- Statutory limitations on FTI access (HS agencies receiving FTI may not HS be part of the outsourcing)
- Timely notification via 45-day contractor notice - should be done as soon as the contract is awarded to ensure security requirements are in place before implementation begins
- Relationship between agencies receiving FTI and the vendor must be established in writing. SLA between FTI recipient agency and state agency that is party to the outsourcing contract is mandatory. Safeguarding language included in all contracts
- Lack of awareness of IRS safeguarding requirements during contract solicitation and awarding processes may impact contract costs. “Compliance with all federal regulatory requirements” is insufficient language - the vendor may not recognize the security requirements of IRC 6103 and Publication 1075

Specific IT Requirements to Consider

- Off-shore access to FTI is prohibited
- Logical and/or physical separation of FTI
- Auditing requirements (Is auditing being done correctly? Who is conducting analysis and oversight of audit logs? How does the FTI recipient agency fit into this picture?)
- Disaster recovery as well as daily/weekly/monthly back-ups (How is it being done? Is FTI commingled? How are back-ups marked? How are they stored? Who has access?)
- Encryption in transit (Within the operating system, application, database configuration, FTI must be encrypted in transit)
- Use of personal and/or contractor owned computers versus government computers to access FTI
- Computer security policies and procedures
- Training requirements for vendors on disclosure awareness and incident reporting
- Number of contractors with access to FTI – “need to know” must be enforced

Questions?

- Email requests for assistance to **safeguardreports@irs.gov**
- Access **www.IRS.GOV** keyword: Safeguards
- Quarterly Phone Forums

Janet Miner

Director, Office of Safeguards

202-622-6807

