

The Fed-State Security Review of IRS Guidelines

Tim Blevins
FTA Annual Meeting
June 5, 2006

What is the TAG Security Subgroup?

- Formed November 2005 by request of FTA-IRS Tactical Advisory Group
- IRS representatives from Wage & Investment, Small Business/Self Employed, Mission Assurance Security Services and Electronic Tax Administration with other resources as needed
- Six states invited by FTA

Who's on it?

- Key IRS representatives by function
- State members to represent all states
 - Balance of size, geography
 - FTA facilitates communications
- State members serve 2-year terms
- A portion of the State members rotate off every year
 - Liaison with TIGERS for technology security related implementations

Data Security Issues

- Participation in Security Summit
- Review of high-level policy
- Determined need for Security Subgroup
 - State information security officers
 - Executive level IRS support
 - Six states plus TIGERS
 - Bi-weekly conference calls

Data Security Issues

- Update of Publication 1075
- Review of system-specific settings (“SCSEMs”) and self-audit tools
- Security of IRS data in state data warehouses
- Pilot strong authentication for MeF
 - Foreign nationals/background checks

Common Security Controls

- Derived from NIST SP 800-53 *Recommended Security Controls for Federal Information Systems*
- Management Controls:
 - Risk Assessment -identify and document all vulnerabilities
 - Planning- includes a Security plan, policies and procedures
 - System and Service Acquisition- adequate security in place for contractors
 - Certification, Accreditation, and Security Assessments- NIST 800-53 detailed requirements

Common Security Controls (cont)

■ Operational Controls

- Personnel Security-Background checks, access authorized
- Physical Security And Environmental Protection
- Contingency Planning- backup, restoration of data, off-site protections, testing of DR plans
- Configuration Management -maintain inventory of hardware and software components, change control system in place
- Maintenance- Periodic, ongoing, tools used, etc
- System and Information Integrity- Correct flaws, protection mechanisms(anti-virus, spam, attacks, etc) accuracy, completeness, validity and authenticity.

Common Security Controls (cont)

■ Operational Controls continued

- Media Protection-in storage, and when disposed
- Incident Response- Plan and staff to deal with anomalies
- Awareness and Training- Communicate security requirements

■ Technical Controls

- Identification and Authorization
- Access Control- need to know, least permissions
- Audit and Accountability- Reports, Monitoring
- System and Communication Protection -boundary controls, application separation, transmission controls, encryption, web environment controls, etc

Any Project Must Follow Controls

- Controls apply to Data Warehouse or Tax Processing of FTI
- Apply to all environments- Development, Test, and Production
- Apply to onsite and offsite deployments
- In addition Data warehouses have some extra requirements- Exhibit 7 of Pub 1075

Data Warehouse Unique Controls

- Risk assessments of the DW environment
- Planning, detailed policies and procedures of the functions of DW, how legacy data will be brought into the DW and cleansed, not subject to disclosure to the public
- Have adequate security controls to block FTI data to contractors not authorized to access
- For Contingency planning, assure DW resources are synchronized and capable of being restored
- DW audit log must capture information on queries submitted
 - actual query being performed
 - Originator of the query
 - relevant time/stamp information

QUESTIONS?

Tim Blevins, Kansas DOR
trb@kdor.state.ks.us
(785)296-5041

Helping to assure the security of
KDOR employees, facilities, and
information systems