Improving Your Safeguards Review Experience

Greg Ricketts
Steve Matteson
IRS Office of Safeguards
June 9, 2014
Agenda

- Safeguarding Federal Tax Information
- IRS Office of Safeguards – Our Mission
- Partnership
- What We Do -- How Can We Assist?
- Safeguard Security Report
- Safeguard Reviews
- Risk Management and the Future of Safeguards
- Questions and Discussion
Internal Revenue Service
Safeguarding Federal Tax Information

- Delegated Authority
- N & U Determinations
- Operational Policy & Procedure

- Manages Relationships between IRS and External Agencies
- Facilitates IRS’ disclosure of Federal tax information (FTI)

- Verification
- Oversight
- Corrective Actions
- Incident Management
Mission:

Promote taxpayer confidence in the integrity of the tax system by ensuring the confidentiality of IRS information provided to federal, state, and local agencies.

Safeguards verifies compliance with Internal Revenue Code 6103(p)(4) safeguard requirements through the identification and mitigation of any risk of loss, breach, or misuse of Federal Tax Information held by external government agencies.
The Office of Safeguards has 300+ agency stakeholders and the number continues to grow with the recent additions of new agency types:

- Federal Agencies
- State Agencies
- Territorial Agencies
- Municipal Agencies
- Tribal Agencies
IRS Office of Safeguards Partnership

- Improve Safeguard Review Experience
- Enhance Communications
- Seek Common Principles
- Integrate Multiple Points of View
- Understand Expectations
- Conduct Face-to-Face Engagements
- Gain Knowledge and Insight
- Share Knowledge and Success Factors
- Identify, Acknowledge, and Address Stakeholder Concerns

Together, we will protect the confidentiality of Federal Tax Information and your Agency’s sensitive information
Under Title 26 U.S. Code Section 6103: *Confidentiality and disclosure of returns and return information*, tax returns and return information are protected from disclosure except in specifically enumerated circumstances

- Returns and return information shall be confidential, and except as authorized by this title, [no one] who has or had access to returns or return information shall disclose any return or return information obtained by him in any manner in connection with his service as an officer or an employee of the United States

- Where disclosure is permitted, section 6103 generally imposes strict safeguarding requirements and requires the IRS to monitor and enforce compliance with those requirements
Safeguards is a necessary program that enhances security through risk management and awareness

- **Cybersecurity Awareness**
  - Most cyber breaches are a result of untrained insiders (employees, contractors, etc.)
  - Risk (or uncertainty) in one’s environment can negatively impact business achievement and success
  - Effective mitigation strategies and controls reduces negative impact to an organization

- **Understanding of Risk**
  - Clear understanding of risk tolerance helps officials set priorities and manage risk consistently throughout the organization allowing the:
    - Allocation of resources
    - Deployment of compensating security measures
    - Awareness of threats and vulnerabilities
How Safeguards Can Help Your Organization

Through safeguarding practices, not only will Federal Tax Information be secure, but the confidentiality of your organization’s assets and data will be further protected.

- Understanding of current threats and vulnerabilities
- Understanding of risk and defining your organization’s risk tolerance
- Enhanced training and security awareness
- Compliance with Federal, State and Commercial standards and best practices
- Documented and implemented physical and information technology security controls
- Sharing of insight and knowledge
  - What works best for similar agencies, culture, and environments?
  - What tools and services are available?
  - What security practices can be shared to reduce operating costs and use of resources?
  - What compensating security controls are available when implementation of requirements is not feasible?
  - What configuration standards and security baselines should be applied?
Provides guidance to ensure the policies, practices, controls, and safeguards employed by recipient agencies, agents, or contractors adequately protect the confidentiality of FTI

Publication 1075 has changed extensively to incorporate feedback from agencies, organizations, IRS and stakeholders

Taking stakeholder feedback into consideration, we changed approximately 85% of the Publication
- Revised formatting of the publication to provide a logical flow of information in a single column format
- Simplified language
- Clarified key definitions, requirements and timelines
- Clarified optional vs. mandatory requirements (e.g. “must” instead of “should”)
- Provided new quick reference charts

Feedback on the Publication 1075 is highly encouraged
Please send any comments, feedback or questions to
SafeguardReports@irs.gov
Develop and maintain a Safeguard Security Report

Review of Safeguard Computer Security Evaluation Matrices (SCSEM)

Utilize a System Development Life Cycle
  ✓ Integrate IT security during systems development and deployment

Ask questions and seek assistance
  ✓ Send questions to the IRS Office of Safeguards mailbox: SafeguardReports@irs.gov
  ✓ Your questions will be forwarded to IRS Subject Matter Experts for research, review, and response
  ✓ Your questions will be answered and taken into consideration for the overall Safeguard program to ensure continued success and minimize any future challenges
Effective in 2014, the Safeguard Security Report (SSR) is the primary source for agencies to report to IRS on the processes, procedures, and security controls in place to protect FTI provided in accordance with IRC 6103(p)(4)

- Annual review of all security controls
  - Enhance the documentation and reporting of the security controls in place to protect FTI
  - Increase IRS awareness of agency security posture and risk level
  - Planned changes can be captured in annual report submissions eliminating the need for report addendums

- Prepares agencies for onsite reviews and enhances continuous monitoring capabilities through a regular review of implemented security controls and requirements at the agency level

- Minimizes redundant documentation and reporting efforts
  - One all encompassing report instead of two reports with redundant information
The objective of system security planning is to improve protection of information system resources

- Safeguard Security Reports are living documents that require periodic review, modification, and plans of action and milestones for implementing security controls
- Describes how the security controls and control enhancements meet Publication 1075 requirements
- Contains sufficient information (including the specification of parameter values for assignment and selection statements either explicitly or by reference) to understand the level of risk
- Will be validated during onsite security control reviews
- Requires head of agency certification and approval
Onsite Safeguards Reviews

- The primary risk identification mechanism for Safeguards is the onsite safeguard review, which assesses the effectiveness of agency controls at protecting FTI.

- Reviews are conducted using Safeguards Computer Security Evaluation Matrices (SCSEMs) and assessment procedures.

- Agency SSR will support onsite evaluation of the Management Operational and Technical (MOT) SCSEM and will greatly reduce time and resources necessary to complete the evaluation.
Safeguard Computer Security Evaluation Matrices (SCSEM)

- Manual test procedures for open box configuration testing of systems that receive, store, process or transmit FTI
- Based on Publication 1075 requirements (NIST 800-53, IRC 6103, Internal Revenue Manuals)
- SCSEMs are posted to the irs.gov web site for agencies to access and review

Automated Testing

- Automating portions of the review provides flexibility to focus on investigating agency-specific scenarios
- Currently use ThreatGuard Secutor Prime SCAP scanner for a sub-set of the system platforms
- Safeguards is moving towards utilizing Nessus for compliance and vulnerability scanning

<table>
<thead>
<tr>
<th>Current Technology SCSEMs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mainframe</strong></td>
</tr>
<tr>
<td>RACF</td>
</tr>
<tr>
<td>ACF2</td>
</tr>
<tr>
<td>Top Secret</td>
</tr>
<tr>
<td>UNISYS</td>
</tr>
<tr>
<td>OpenVMS</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Network Devices</strong></th>
<th><strong>Other Platforms</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Routers</td>
<td>Oracle DBMS</td>
</tr>
<tr>
<td>Cisco Switch</td>
<td>SQL Server DBMS</td>
</tr>
<tr>
<td>Firewall</td>
<td>Fast Enterprises GenTax</td>
</tr>
<tr>
<td>Virtual Private Networks (VPN)</td>
<td>RSI Revenue Premier*</td>
</tr>
<tr>
<td>Novell Netware</td>
<td>Oracle Enterprise Tax &amp; Policy Mgmt*</td>
</tr>
<tr>
<td>Wireless Local Area Network (LAN)</td>
<td>Teradata Data Warehouse*</td>
</tr>
<tr>
<td>Network Assessment</td>
<td>Multi-Functional Devices</td>
</tr>
<tr>
<td></td>
<td>MOT</td>
</tr>
</tbody>
</table>
Minimize time and resources of onsite reviews while obtaining a greater understanding of system risk and vulnerabilities

- Uses a remote scanning execution method
- Logs into Unix and Windows servers, Cisco devices, SCADA systems, IBM iSeries servers, and databases to determine if they have been configured in accordance with Pub 1075
- Scanning is credentialed
- Vulnerability and compliance information will be obtained at one time
- Knowing how a server is configured, how it is patched and what vulnerabilities are present can help determine measures to best mitigate risk
- Identify vulnerabilities during onsite reviews
  - Recommended actions are provided to support remediation
  - For each review finding the evaluated risk for potential loss, breach, or misuse of FTI establishes the targeted implementation date based on the recommended timeframe for resolution in the chart below:

<table>
<thead>
<tr>
<th>Risk Category</th>
<th>Associated Timeframe for Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>3 months from the date of the review closing conference</td>
</tr>
<tr>
<td>Significant</td>
<td>6 months from the date of the review closing conference</td>
</tr>
<tr>
<td>Moderate</td>
<td>9 months from the date of the review closing conference</td>
</tr>
<tr>
<td>Limited</td>
<td>12 months from the date of the review closing conference</td>
</tr>
</tbody>
</table>

- Security Reporting
  - Vulnerabilities are tracked in agency specific Corrective Action Plans (CAP) or Plan of Action and Milestones until fully implemented
  - Annual Safeguard Security Report reporting
Safeguards
Risk Management

Continuous Reporting Requirements
- Maintain agreements
- Bi-annual Corrective Action Plan
- Annual SSR
- Once every 3 years onsite review

Request FTI / Data Sharing Agreement

Develop Safeguard Security Report (SSR)

Monitor Controls
Vulnerabilities tracked in agency specific Corrective Action Plan (CAP) until fully mitigated

Implement Security Controls

Assess Security Controls
Annually via agency procedures, and at least once every 3 years by IRS Office of Safeguards
The IRS Office of Safeguards is transitioning to a risk management model based on:

- Compensating security controls and measures
- Continuous monitoring and agency self-reporting
- Enabling success of your organization's and programs while realizing the significance and importance of security

This transition will not only improve the onsite review process but will minimize redundant reporting efforts while enhancing the physical and electronic protection of FTI

Your opinions, comments and feedback matter

Our office is dedicated to customer service and promoting safeguarding of sensitive information and IT security best practices
Questions and Discussion

Greg Ricketts  
Director  
IRS Office of Safeguards  
Email: Gregory.T.Ricketts@irs.gov  
Office: (901) 546-3078  
Work cell: (901) 600-3016

Steve Matteson  
Senior Technical Advisor  
IRS Office of Safeguards  
Email: Steven.M.Matteson@irs.gov  
Office/Cell: 214-784-5128

SafeguardReports@irs.gov