Electronic Transaction Risk Assessment

Tony Trenkle

Social Security Administration

Social Security Service Challenges

- Receive 240 million earnings items from 6.5 million employers
- Send out 125 million Social Security Statements
- Issue 16 Million SS Cards
- Give benefits to 50 Million People
- Answer 60 million 800-number calls
- …*with a downsized workforce.*

SSA’s Web Experience

Social Security Online

- *SSA Online* - May 1994
- FY 99 Customers - 8.5 million
- FY 00 customers-13 mil.
- Mostly informational services
- Limited transaction services

SSA’s Online PEBES Experience

- PEBES - “Personal Earnings and Benefit Estimate Statement”
- **Online PEBES (interactive version)**
  - 71,000 requested while service available
  - about 93% opted for online response
- PEBES Aftermath-Lessons Learned

SSA’s Current Internet Strategy

- Continue to build informational services
- Create an attractive, navigable environment that allows easy online transactions.
- Develop options for business partners
- For general public provide:
  - Suites of Services
  - Customer Account.
- Integrate with other customer service channels.

Why Risk Assessment?

- Government Paperwork Elimination Act
  - Legislative mandate requires agencies by 2003 to allow customers the option to submit information or transact electronically, when practicable.
  - Risk assessments required
- SSA move to electronic services
  - Need to define proper authentication strategy
  - Lessons learned from PEBES

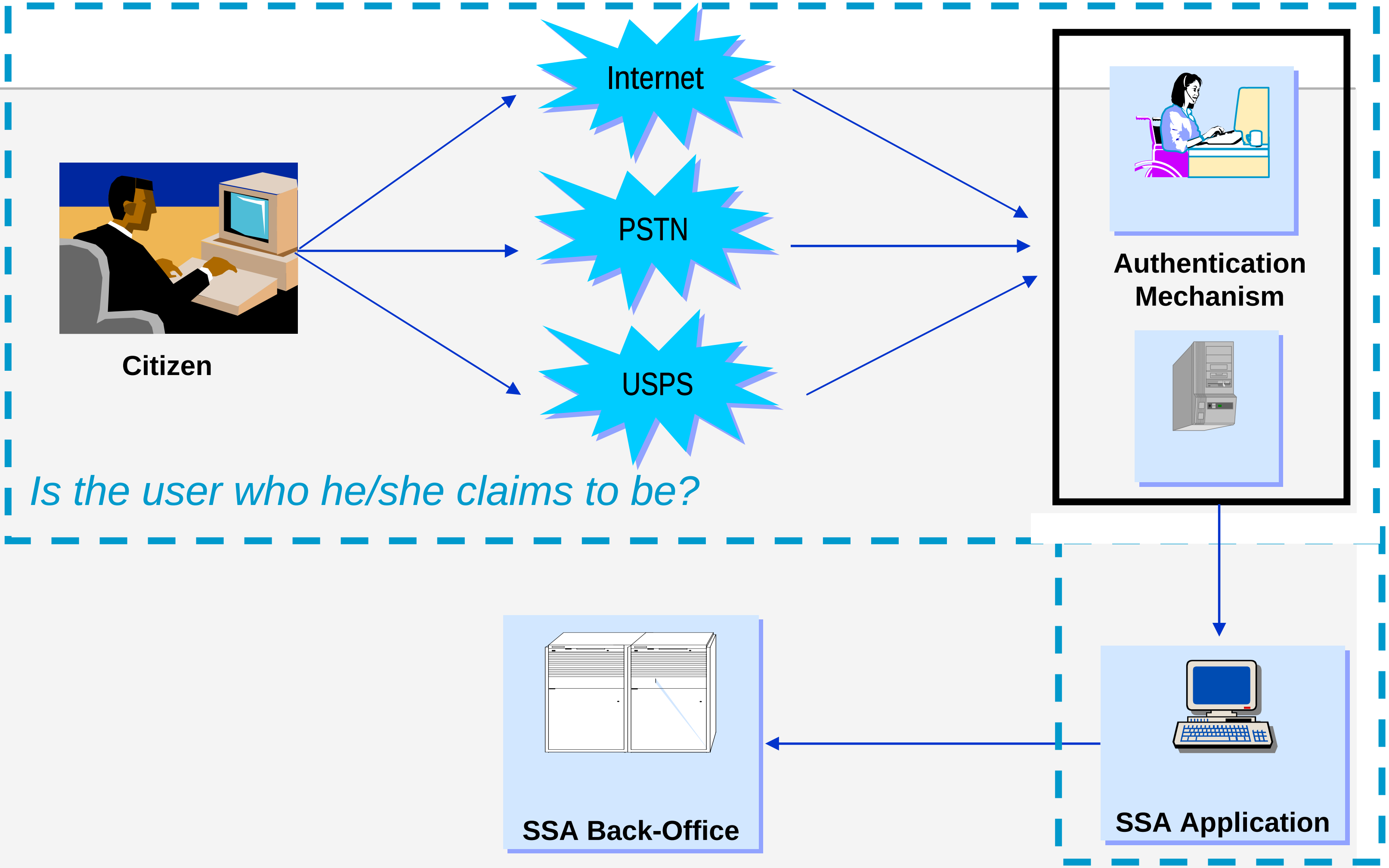
Risk Management Assessment

- SSA identified three risks:
  - Improper disclosure
  - Program Fraud
  - Image
- Assess the electronic transaction risks
  - Recommend an “appropriate” authentication mechanism for a given transaction
  - Examine transactions in three media
  - Provide rough cost estimates
- Examine Best Practices

Risk Management Assessment

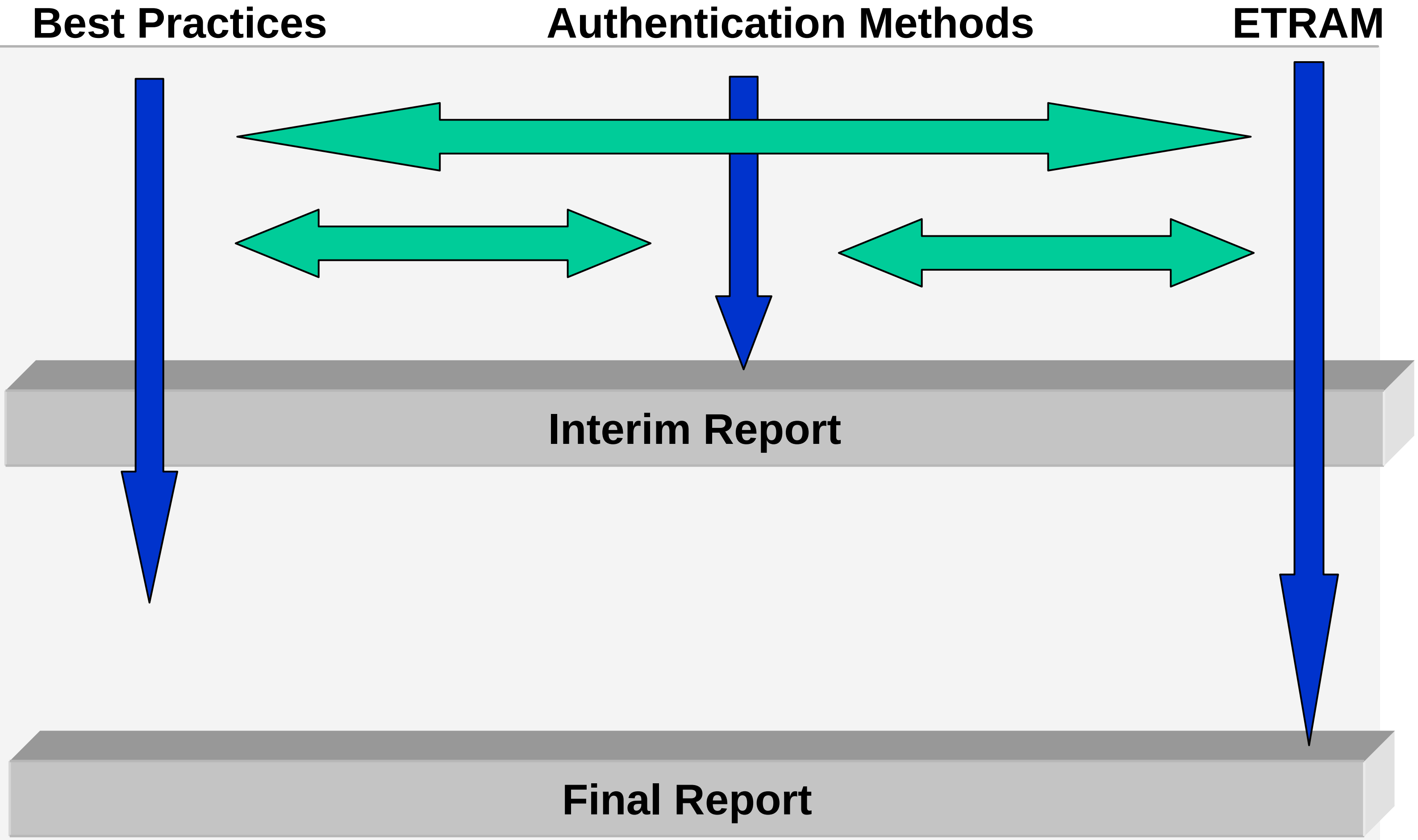
- Develop a methodology for determining application risk
- Use the methodology as a tool to choose appropriate authentication technology
- Test on several applications.
- Contract Awarded under ACES to DST/CSC

Project Scope



Is the user who he/she claims to be?

Project Plan



Best Practices

Authentication Methods

ETRAM

Interim Report

Final Report

Best Practices

- GAO Report, *InfoSec Risk Assessment: Practices of Leading Organizations*
- Searched proprietary database containing over one hundred organizations
  - No examples of a focused ETRA were found, mostly general risk assessments
  - Selected two representative cases--one from public sector and one from private sector--that illustrate range of approaches
  - Selected two cases to validate GAO findings
- Examined a total of eight cases in detail

Findings

- Few, if any, organizations have performed ETRAs *before* implementing a new authentication method
- Identified six “best practices” of overall risk assessments
- Most organizations currently use PIN/Password
- Other methods, notably software-based client keys are becoming more common
- There are no widely-accepted industry cost models

Six “Best Practices” from General Risk Assessments

- Involve business and technology experts
- Integrate tools to facilitate the process
- Fully document results
- Clearly define risk assessment leaders
- Involve senior management
- Narrow focus of assessments

Other Risks and Costs Need to be Considered in Final Decision

- Identification risk
- Back-End risk- database of passwords
- Risk over time
  - Single vs. multiple transactions
- Interoperability (GPEA guideline)
  - Intra-agency, inter-agency, B2G, C2G
- Infrastructure and O&M costs
  - Helpdesk, databases, repositories...

Summary of Internet Authentication Risks

This analysis is for end-to-end authentication for a single transaction.

	Risk			
Application Level End-to-End Auth. Mechanism	**HTTP only No SSL**	**SSL with No Certificates**	**SSL with Server Certificate Only**	**SSL with Server & Client Certificates**
None	VERY HIGH	VERY HIGH	VERY HIGH	LOW
Reusable Password	HIGH	MEDIUM	LOW	LOW
Use Once Password	HIGH	MEDIUM	LOW	LOW
SW One Time Password	MEDIUM	MEDIUM	LOW	LOW
HW One Time Password	MEDIUM	MEDIUM	LOW	LOW
Biometrics	HIGH	MEDIUM	LOW	LOW

Risks of Telephone Authentication Methods

Type of Risk	**Basic Four C/R**	**Multiple Random C/R**	**Multiple Random C/R and Caller ID or Dial Back**	**Dial Back or Caller ID**	**Educate Staff and Disable Unneeded Voice Mail**
False identity of caller; caller initiated	HIGH	LOW	VERY LOW	MEDIUM	MEDIUM
False identity of unknown customer; SSA initiated	HIGH	LOW	VERY LOW	N/A	MEDIUM
False identity of known customer; SSA initiated	MEDIUM	LOW	VERY LOW	N/A	MEDIUM

Risks of Postal Mail Authentication Methods

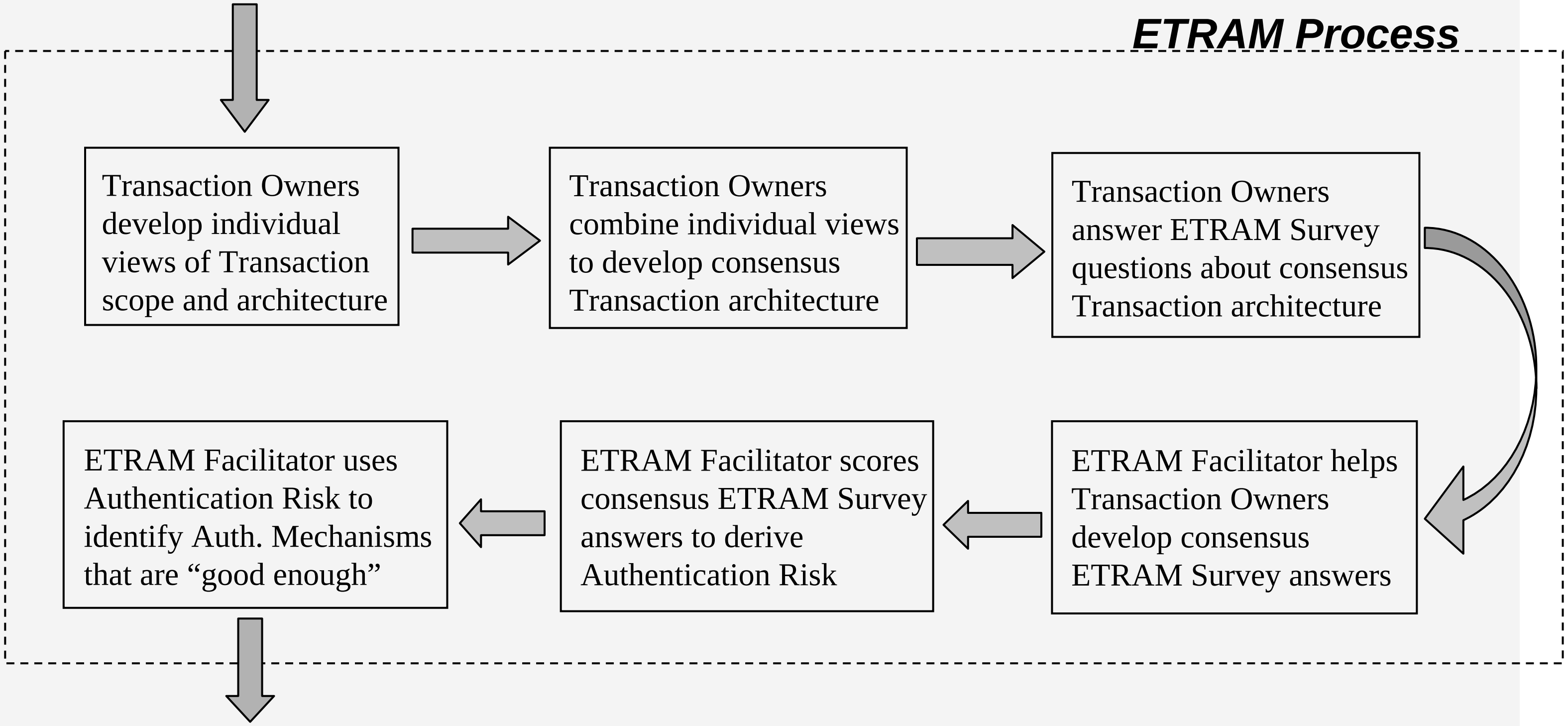
Type of Risk	First-Class Mail	Certified Mail with Return Receipt	Registered Mail with Return Receipt	Restricted Mail
Delivery to wrong address	HIGH	MEDIUM	MEDIUM	LOW
Delivery to wrong person	HIGH	MEDIUM	MEDIUM	LOW

ETRAM Description

- ETRAM consists of:
  - An Authentication Risk Model (ARM) that provides the framework for the assessment
  - A survey that is given to transaction owners to determine the risks associated with a given transaction
  - A process for administering the survey, generating consensus answers, scoring the survey, and selecting an authentication mechanism

ETRAM Process

SSA Identifies Transaction



ETRAM Process

Transaction Owners develop individual views of Transaction scope and architecture

Transaction Owners combine individual views to develop consensus Transaction architecture

Transaction Owners answer ETRAM Survey questions about consensus Transaction architecture

ETRAM Facilitator helps Transaction Owners develop consensus ETRAM Survey answers

ETRAM Facilitator scores consensus ETRAM Survey answers to derive Authentication Risk

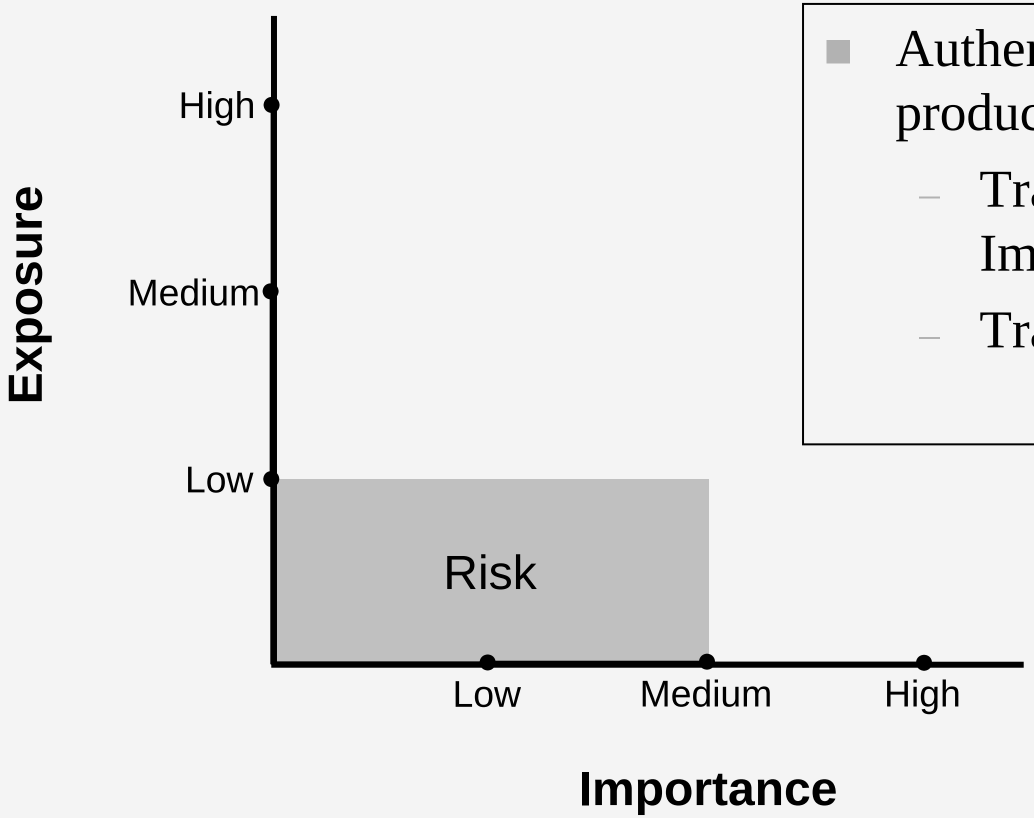
ETRAM Facilitator uses Authentication Risk to identify Auth. Mechanisms that are “good enough”

SSA uses Authentication Mechanisms as starting point for policy decision

The ETRAM Survey

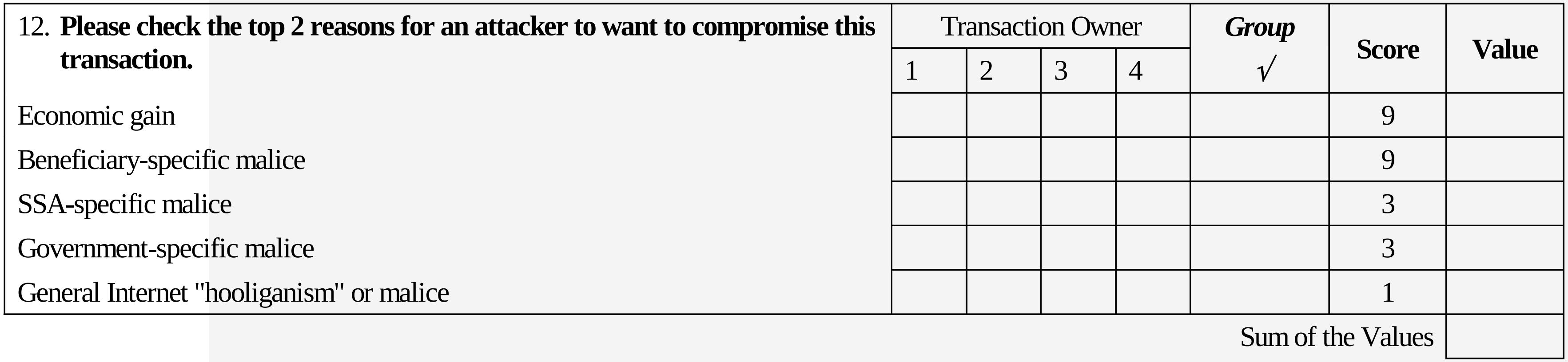
- 22 questions-some multiple answers
- Designed to provide measures for five variables that are inputs into ARM
  - Value
  - Damage
  - Motivation
  - Opportunity
  - Protection

ETRAM Authentication Risk Model



- Authentication Risk is the product of
  - Transaction Importance
  - Transaction Exposure

Sample Question from Survey



12. **Please check the top 2 reasons for an attacker to want to compromise this transaction.**	Transaction Owner				***Group***	**Score**	**Value**
	1	2	3	4	√		
Economic gain						9	
Beneficiary-specific malice						9	
SSA-specific malice						3	
Government-specific malice						3	
General Internet "hooliganism" or malice						1	
						Sum of the Values	

Possible Next Steps for SSA

- Make survey automated and Web-based
- Allow Importance and Exposure to have different weights
- Account for interactions among survey questions
- Refine survey and add new questions
- Explicitly consider risks of customer IT systems
- Extend ETRAM to consider “back-end” processing of a transaction
- Explore development of an “authentication portal” that provides single sign-on for visitors to www.ssa.gov

Summary

- ETRAM is a structured methodology to help SSA to make robust and well-informed authentication policy decisions for electronic transactions.
- ETRAM helps SSA meet the requirements of GPEA.
- Other agencies should piggyback off of SSA’s work to develop their own ETRAM.
- ETRAM is an evolving tool, not a panacea.