U.S. DEPARTMENT OF
HEALTH & HUMAN SERVICES

CMS
CENTERS for MEDICARE & MEDICAID SERVICES

Cultivating a Training and Awareness Program: From Seedling to Sapling

Julie Boughn
Director,
Division of CMS Enterprise Standards

Environment & History

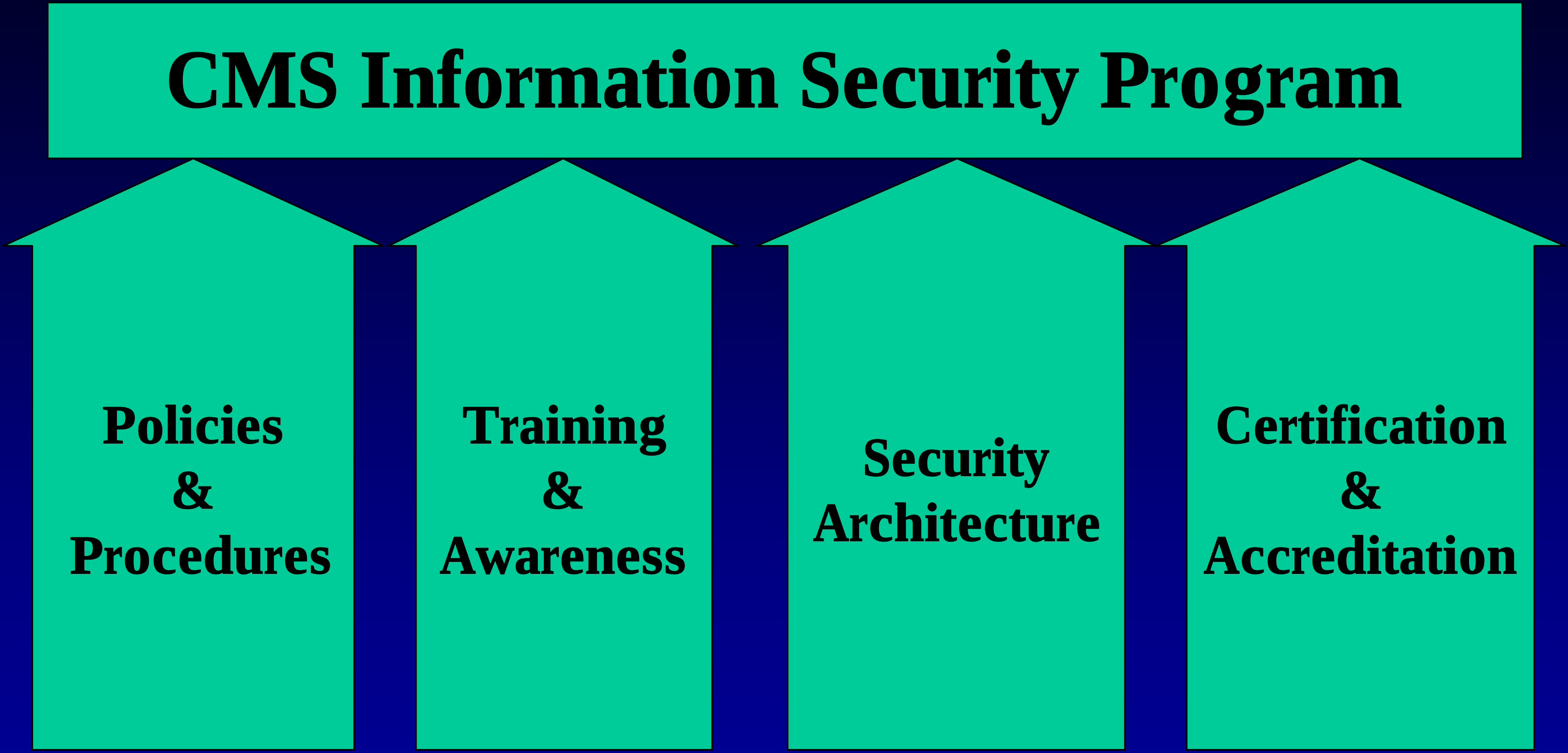
- Centers for Medicare & Medicaid Services (CMS)

  (formerly the Health Care Financing Administration [HCFA])
- Medicare
- Medicaid
- State Children's Health Insurance Program (SCHIP)

CMS - Bird’s Eye View (FY2001)

- Personnel – 4,600 government employees
- Beneficiaries – 78 million
- Benefit Outlays - $359 billion
- Program Management - $2.29 billion
- Medicare Fiscal Intermediaries and Carriers – approximately 70

4 Pillars of the IT Security Program



CMS Information Security Program

Policies & Procedures

Training & Awareness

Security Architecture

Certification & Accreditation

CMS Security Organization

Where Did We Start ???

- Current Awareness & Training Report
- Awareness & Training Structure Report
- Framework Report
- Program Details
- Senior Executives Briefing

Training and Awareness

- Target Audiences
  - Management/Executives
  - End Users (include contractors)
  - System Developers/Maintainers

- Message Delivery
  - Formal briefings & classes
  - Awareness Day
  - Conferences
  - Cyber Tyger
  - Web
  - Newsletter
  - Computer Based Training

Senior Executive & Manager's briefings

- Available on NIST FASP site (http://csrc.nist.gov/fasp/)
- Must have Executive and Managers support
- Simple
- Non-technical
- Peer led round-table discussion
- Publicize their Information Resources

ISSO & SSP courses

- Senior management backing
- Peer led round-table discussion
- Prepare for resistance
- Must provide continuous support resources
- Must provide “TOOLS”

“TOOLS” - Security in the SDLC

System Security Levels

Business Case Analysis

Accept. Risk Safeguards

System Req. Document

Threat ID Resource

Identify Vulnerabilities

RA & SSP

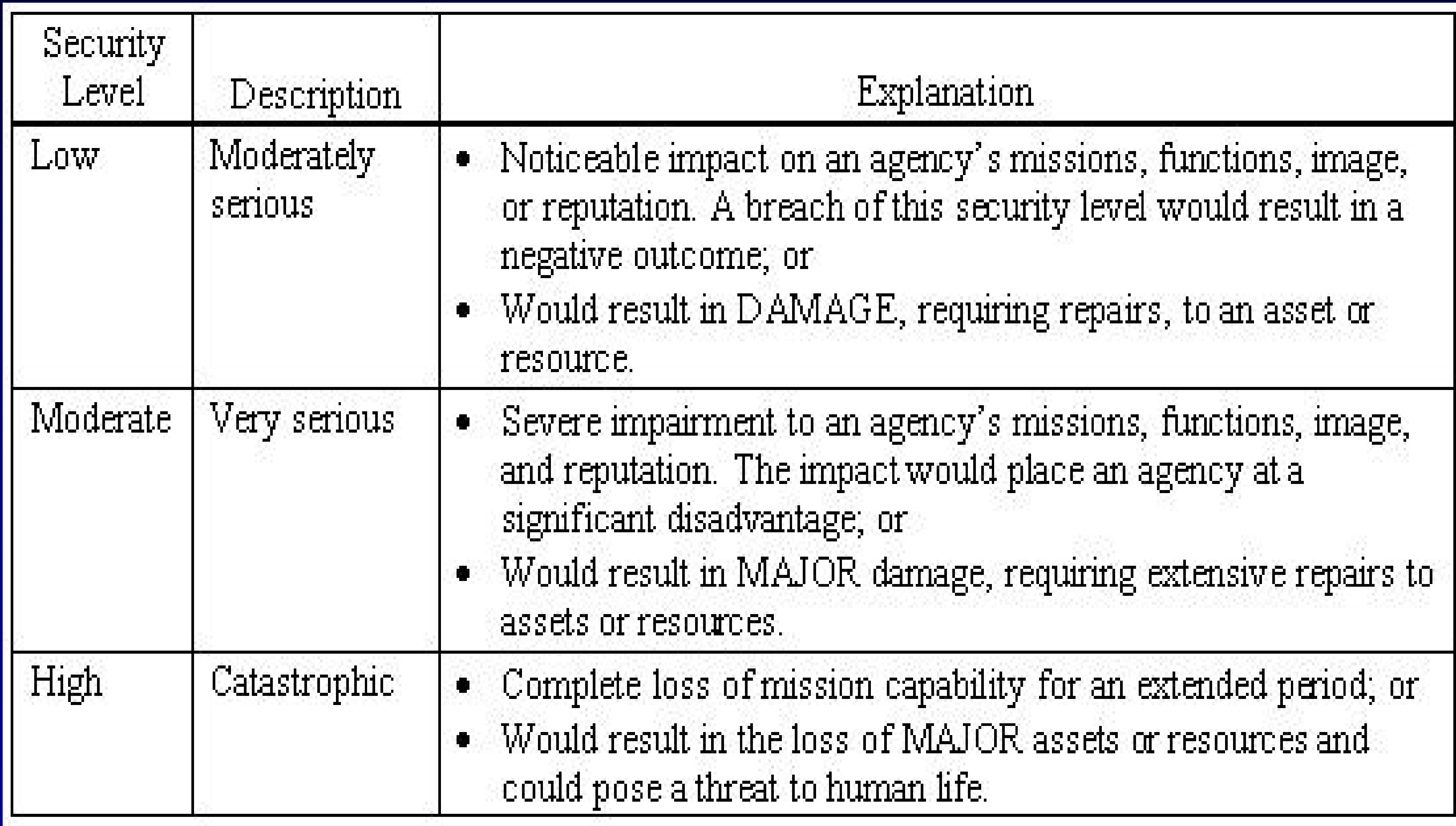
Legend

Security Deliverables

Resources

System Development "TOOLS"

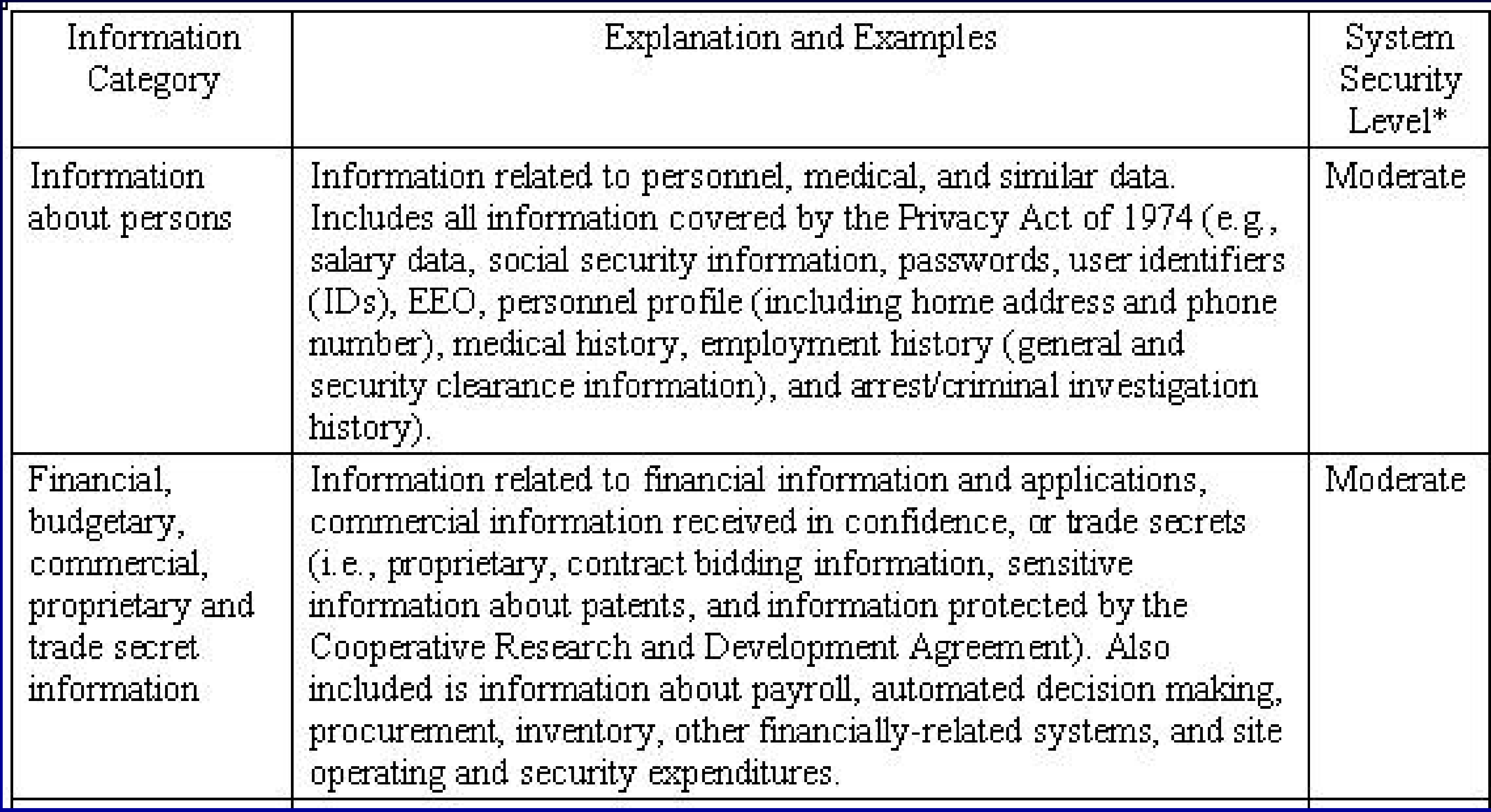
System Security Levels (SSL)



Security Level	Description	Explanation
Low	Moderately serious	• Noticeable impact on an agency's missions, functions, image, or reputation. A breach of this security level would result in a negative outcome; or • Would result in DAMAGE, requiring repairs, to an asset or resource.
Moderate	Very serious	• Severe impairment to an agency's missions, functions, image, and reputation. The impact would place an agency at a significant disadvantage; or • Would result in MAJOR damage, requiring extensive repairs to assets or resources.
High	Catastrophic	• Complete loss of mission capability for an extended period; or • Would result in the loss of MAJOR assets or resources and could pose a threat to human life.

System Development “TOOLS”

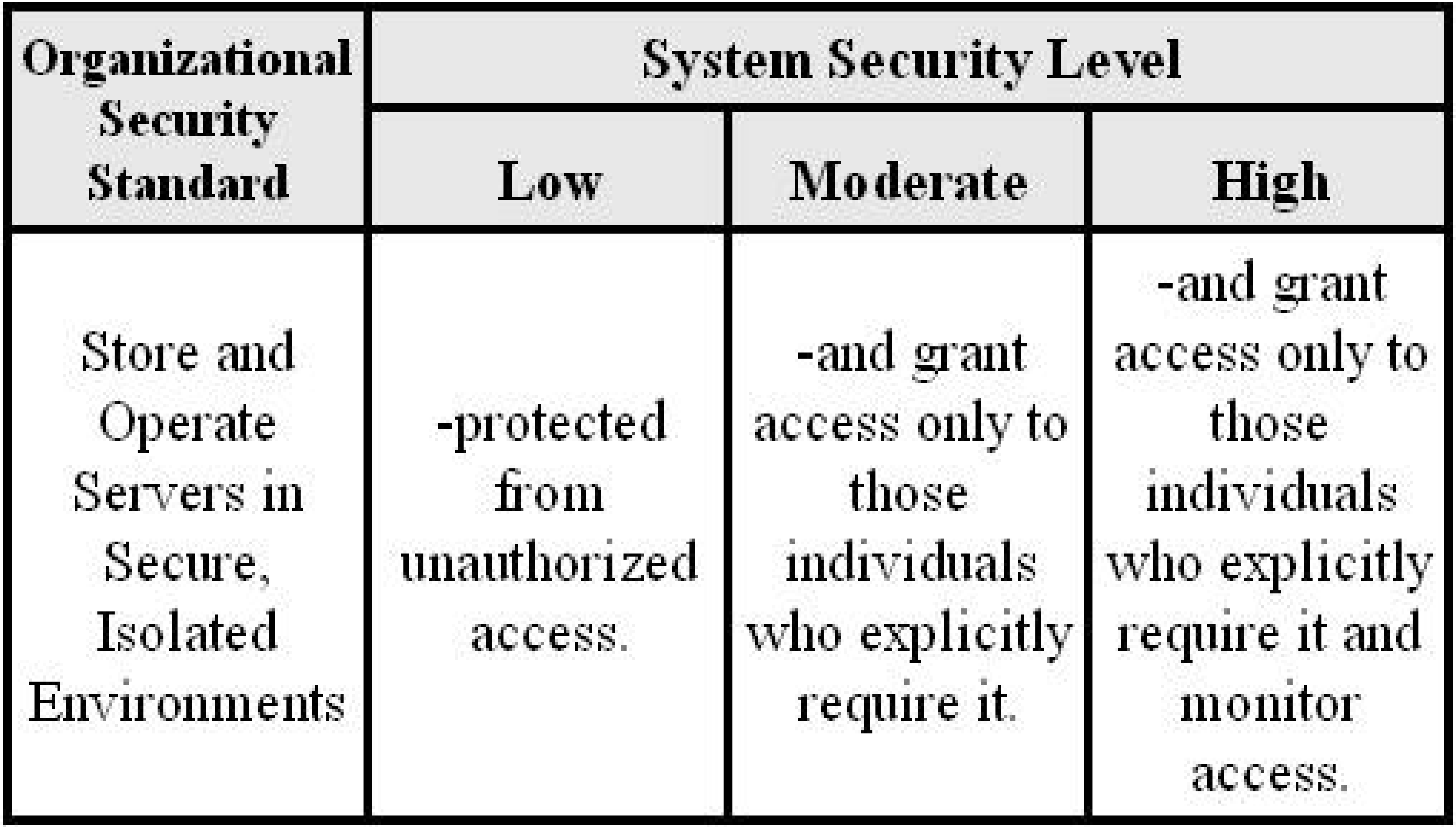
SSL - Information Categories



Information Category	Explanation and Examples	System Security Level*
Information about persons	Information related to personnel, medical, and similar data. Includes all information covered by the Privacy Act of 1974 (e.g., salary data, social security information, passwords, user identifiers (IDs), EEO, personnel profile (including home address and phone number), medical history, employment history (general and security clearance information), and arrest/criminal investigation history).	Moderate
Financial, budgetary, commercial, proprietary and trade secret information	Information related to financial information and applications, commercial information received in confidence, or trade secrets (i.e., proprietary, contract bidding information, sensitive information about patents, and information protected by the Cooperative Research and Development Agreement). Also included is information about payroll, automated decision making, procurement, inventory, other financially-related systems, and site operating and security expenditures.	Moderate

System Development “TOOLS”

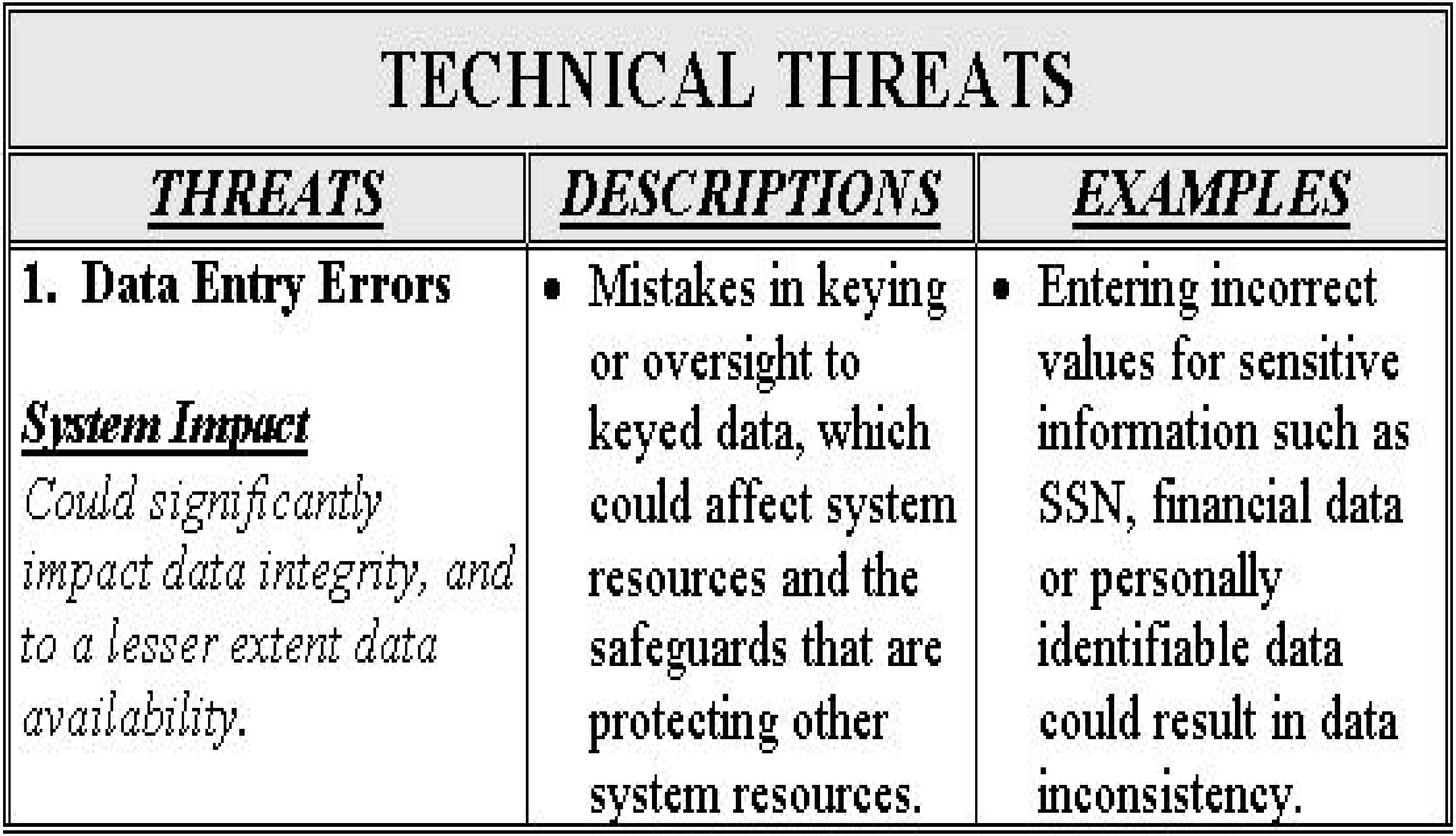
Acceptable Risk Safeguards



Organizational Security Standard	System Security Level		
	Low	Moderate	High
Store and Operate Servers in Secure, Isolated Environments	-protected from unauthorized access.	-and grant access only to those individuals who explicitly require it.	-and grant access only to those individuals who explicitly require it and monitor access.

System Development "TOOLS"

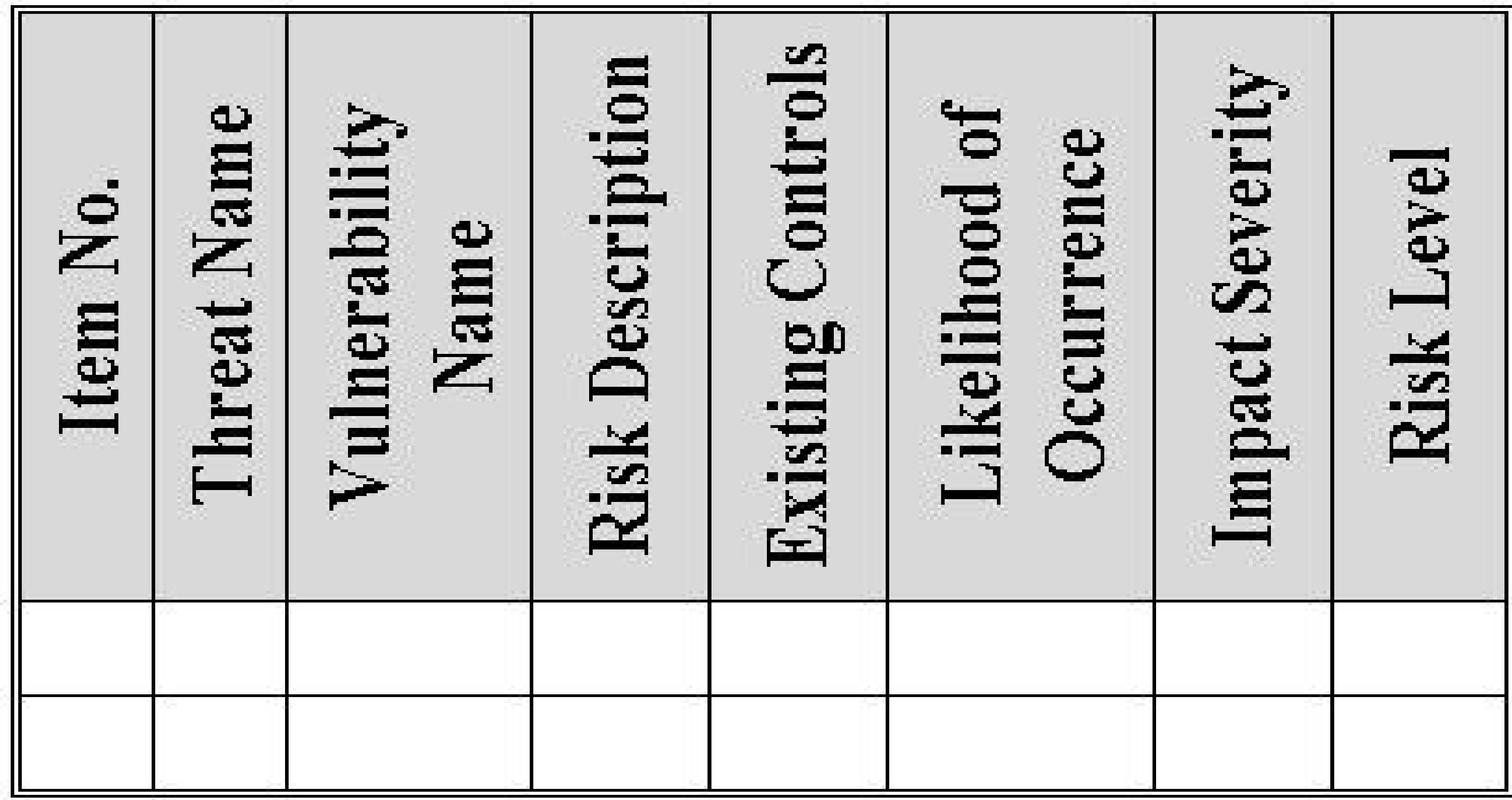
Threat Identification Resource



TECHNICAL THREATS		
THREATS	***DESCRIPTIONS***	***EXAMPLES***
1. Data Entry Errors ***System Impact*** *Could significantly impact data integrity, and to a lesser extent data availability.*	• Mistakes in keying or oversight to keyed data, which could affect system resources and the safeguards that are protecting other system resources.	• Entering incorrect values for sensitive information such as SSN, financial data or personally identifiable data could result in data inconsistency.

System Development “TOOLS”

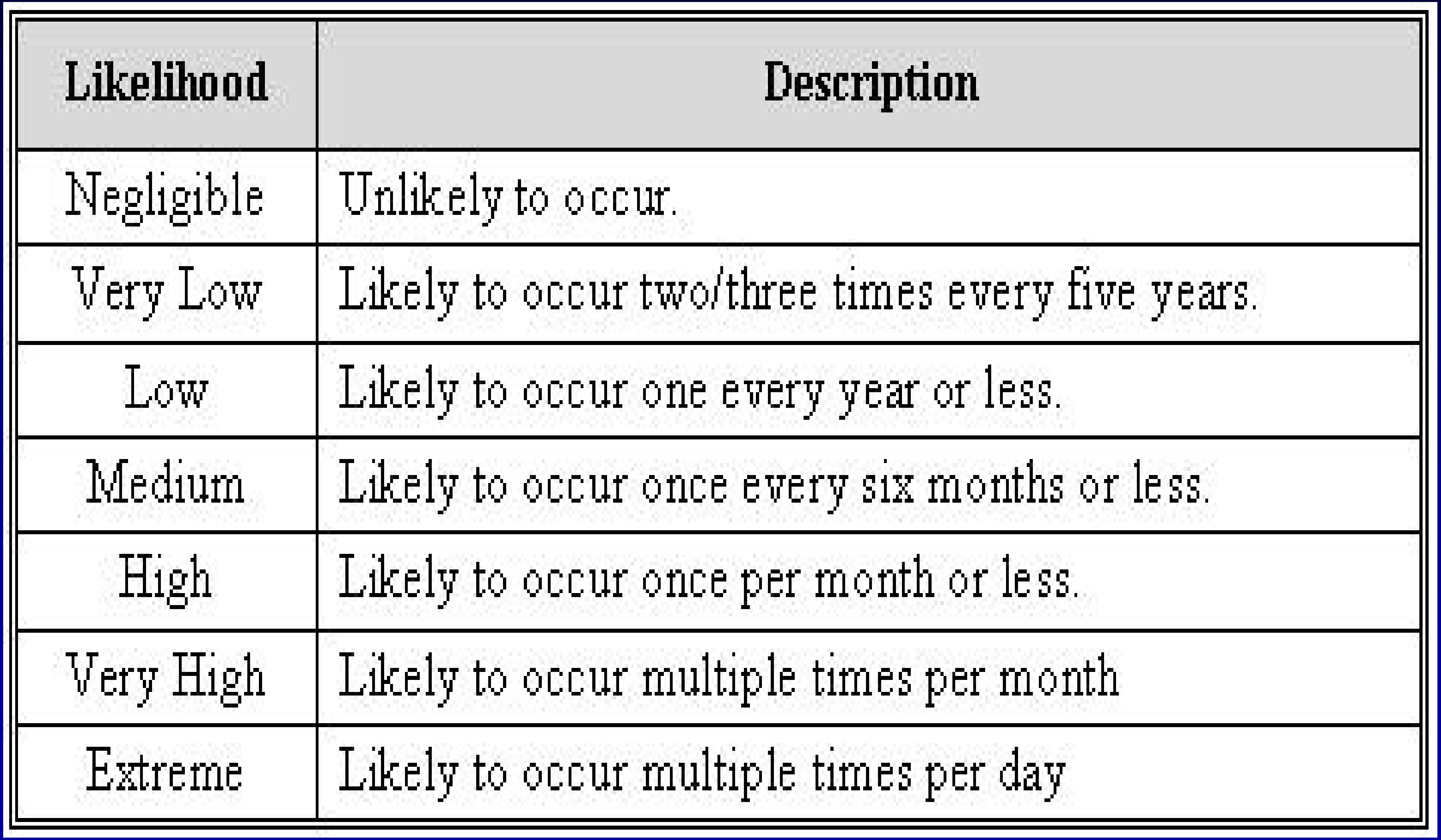
RA – Risk Determination



Item No.	Threat Name	Vulnerability Name	Risk Description	Existing Controls	Likelihood of Occurrence	Impact Severity	Risk Level

System Development "TOOLS"

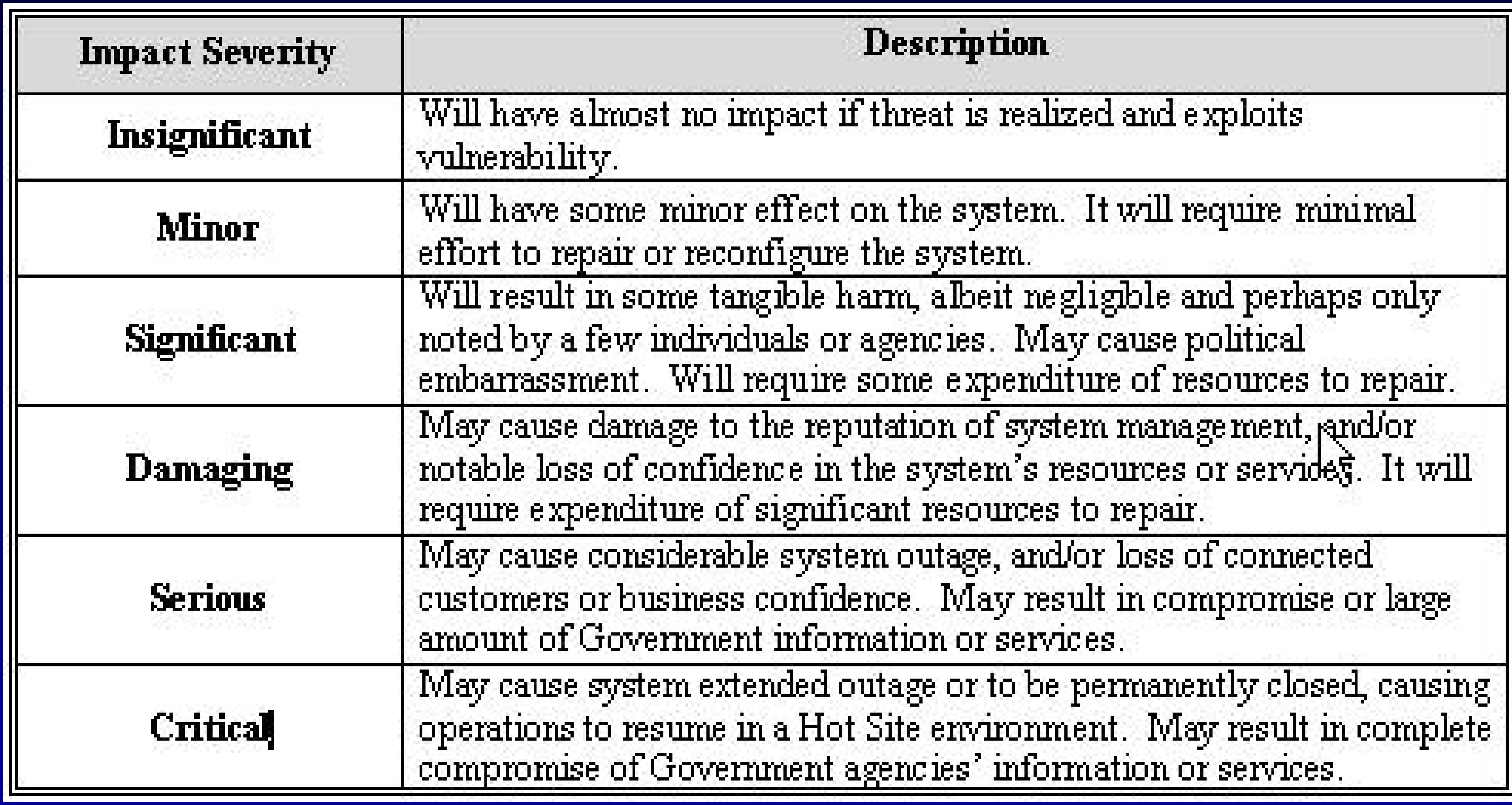
RA – Likelihood of Occurrence



Likelihood	Description
Negligible	Unlikely to occur.
Very Low	Likely to occur two/three times every five years.
Low	Likely to occur one every year or less.
Medium	Likely to occur once every six months or less.
High	Likely to occur once per month or less.
Very High	Likely to occur multiple times per month
Extreme	Likely to occur multiple times per day

System Development "TOOLS"

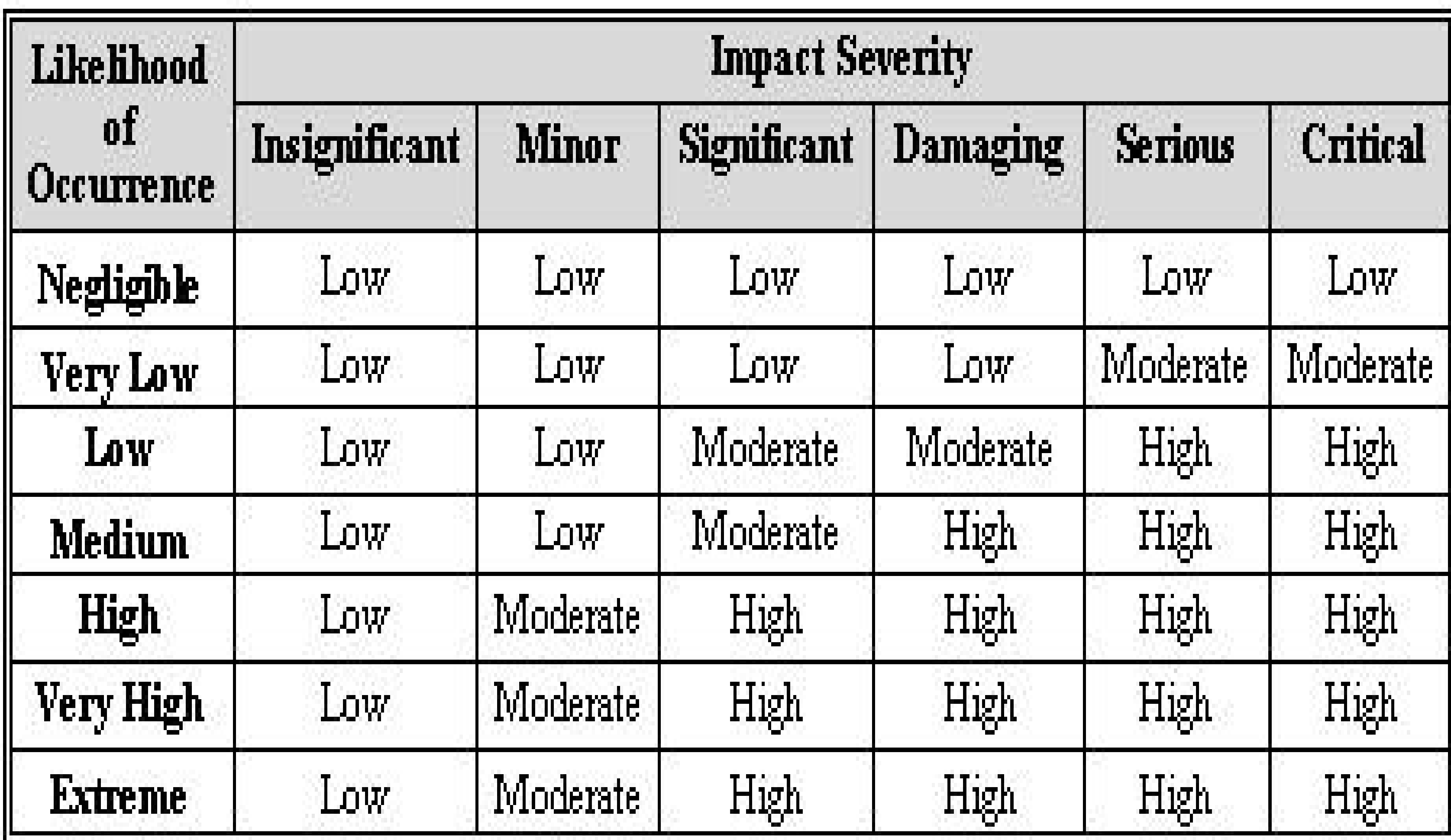
RA – Impact Severity Levels



Impact Severity	Description
Insignificant	Will have almost no impact if threat is realized and exploits vulnerability.
Minor	Will have some minor effect on the system. It will require minimal effort to repair or reconfigure the system.
Significant	Will result in some tangible harm, albeit negligible and perhaps only noted by a few individuals or agencies. May cause political embarrassment. Will require some expenditure of resources to repair.
Damaging	May cause damage to the reputation of system management, and/or notable loss of confidence in the system's resources or services. It will require expenditure of significant resources to repair.
Serious	May cause considerable system outage, and/or loss of connected customers or business confidence. May result in compromise or large amount of Government information or services.
Critical	May cause system extended outage or to be permanently closed, causing operations to resume in a Hot Site environment. May result in complete compromise of Government agencies' information or services.

System Development "TOOLS"

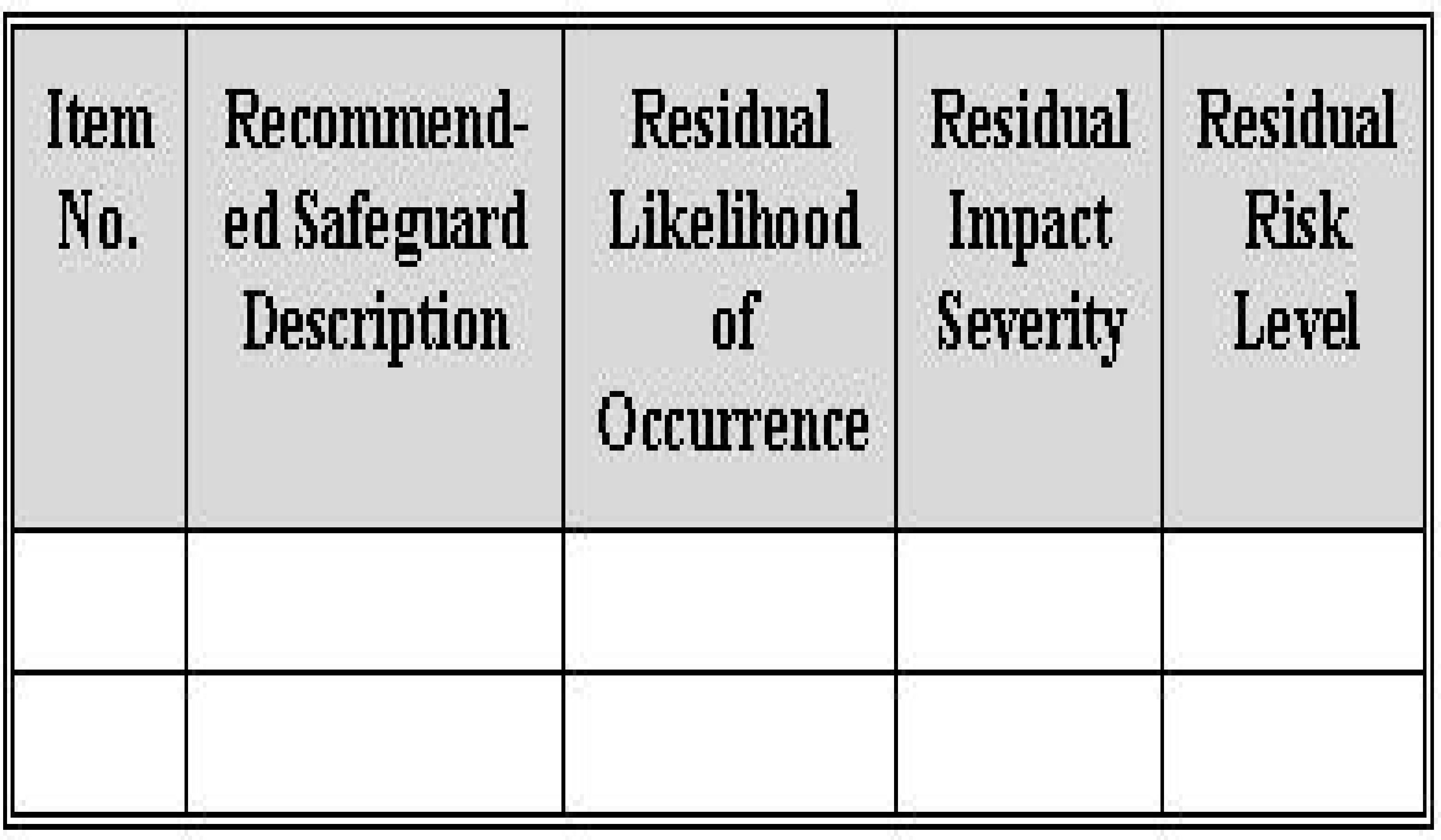
RA – Risk Levels



Likelihood of Occurrence	Impact Severity					
	Insignificant	Minor	Significant	Damaging	Serious	Critical
Negligible	Low	Low	Low	Low	Low	Low
Very Low	Low	Low	Low	Low	Moderate	Moderate
Low	Low	Low	Moderate	Moderate	High	High
Medium	Low	Low	Moderate	High	High	High
High	Low	Moderate	High	High	High	High
Very High	Low	Moderate	High	High	High	High
Extreme	Low	Moderate	High	High	High	High

System Development “TOOLS”

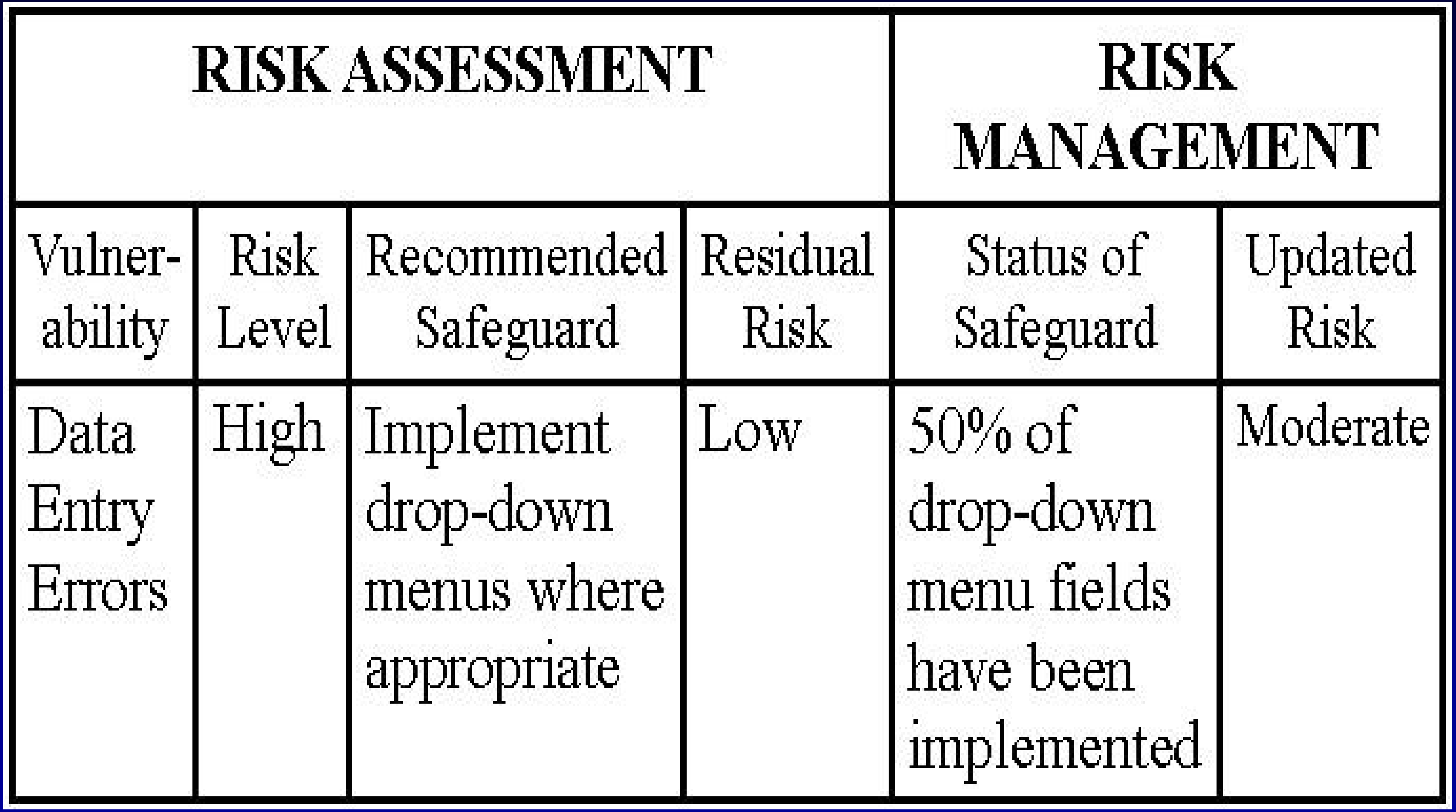
RA – Safeguards Determination



Item No.	Recommend-ed Safeguard Description	Residual Likelihood of Occurrence	Residual Impact Severity	Residual Risk Level

System Development “TOOLS”

Risk – Mitigating Actions



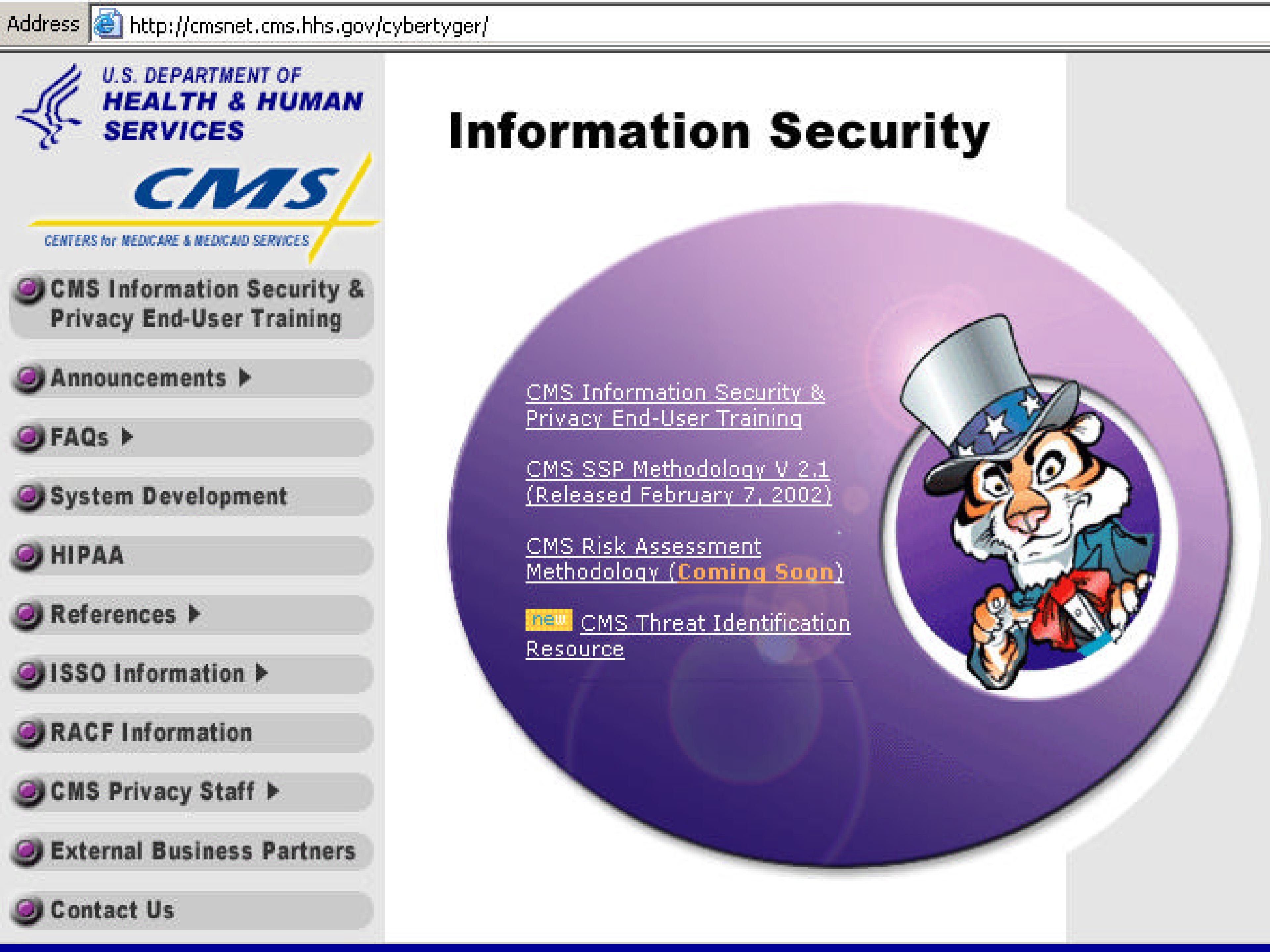
RISK ASSESSMENT				RISK MANAGEMENT	
Vulner-ability	Risk Level	Recommended Safeguard	Residual Risk	Status of Safeguard	Updated Risk
Data Entry Errors	High	Implement drop-down menus where appropriate	Low	50% of drop-down menu fields have been implemented	Moderate

Awareness Days & Conferences

- Target audiences
- Publicity
- Free-trinkets
- Format & time allocations
- Don’t be afraid to try something new

Cyber Tyger

- Everything’s coming up “Cyber Tygers”
- CyberTyger@cms.hhs.gov


Address
http://cmsnet.cms.hhs.gov/cybertyger/
U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES
CMS
CENTERS for MEDICARE & MEDICAID SERVICES
CMS Information Security & Privacy End-User Training
Announcements ▶
FAQs ▶
System Development
HIPAA
References ▶
ISSO Information ▶
RACF Information
CMS Privacy Staff ▶
External Business Partners
Contact Us

Information Security

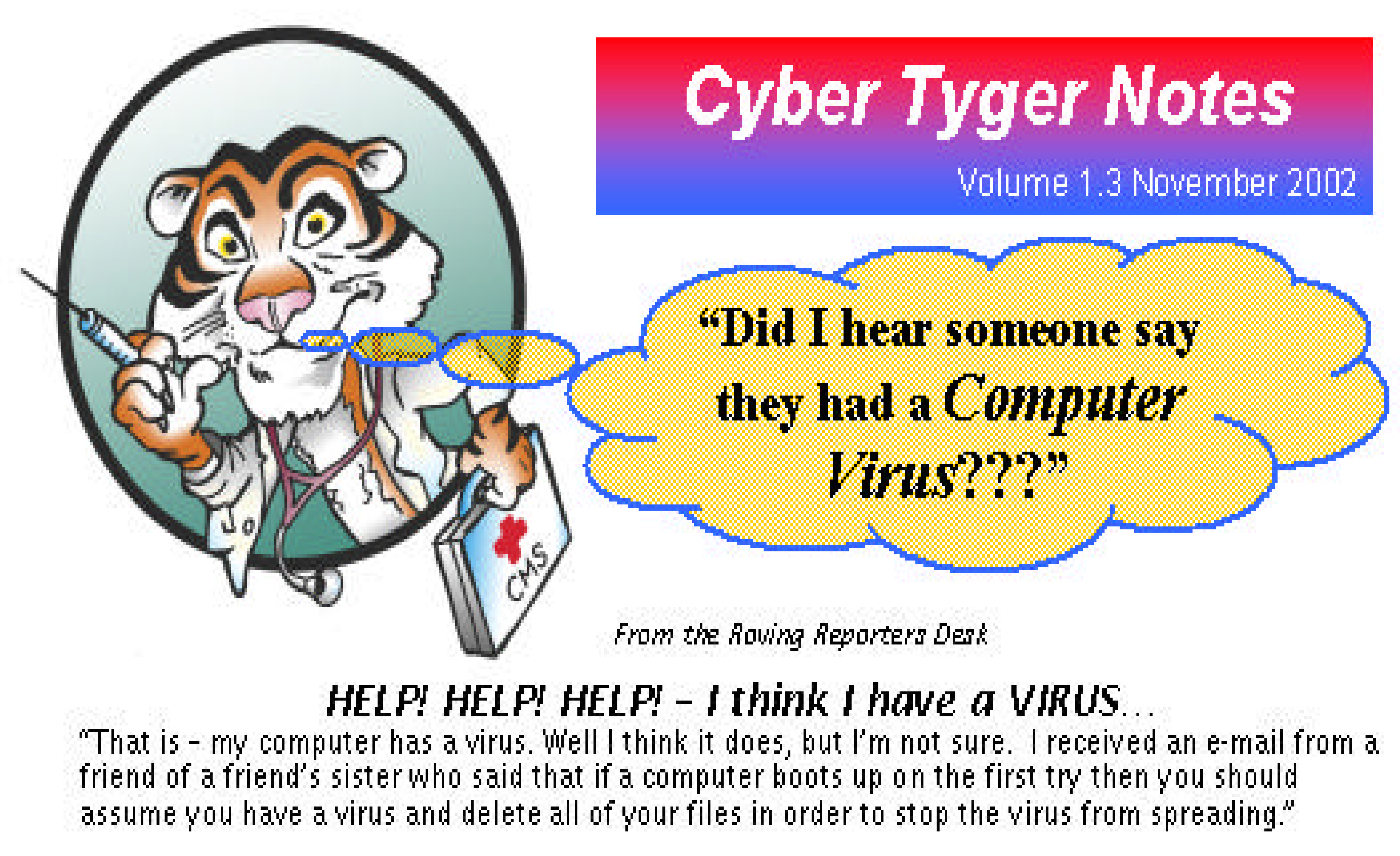
CMS Information Security & Privacy End-User Training

CMS SSP Methodology V 2.1 (Released February 7, 2002)

CMS Risk Assessment Methodology (**Coming Soon**)

new CMS Threat Identification Resource

Cyber Tyger Notes



Cyber Tyger Notes

Volume 1.3 November 2002

"Did I hear someone say they had a *Computer Virus*???"

From the Roving Reporters Desk

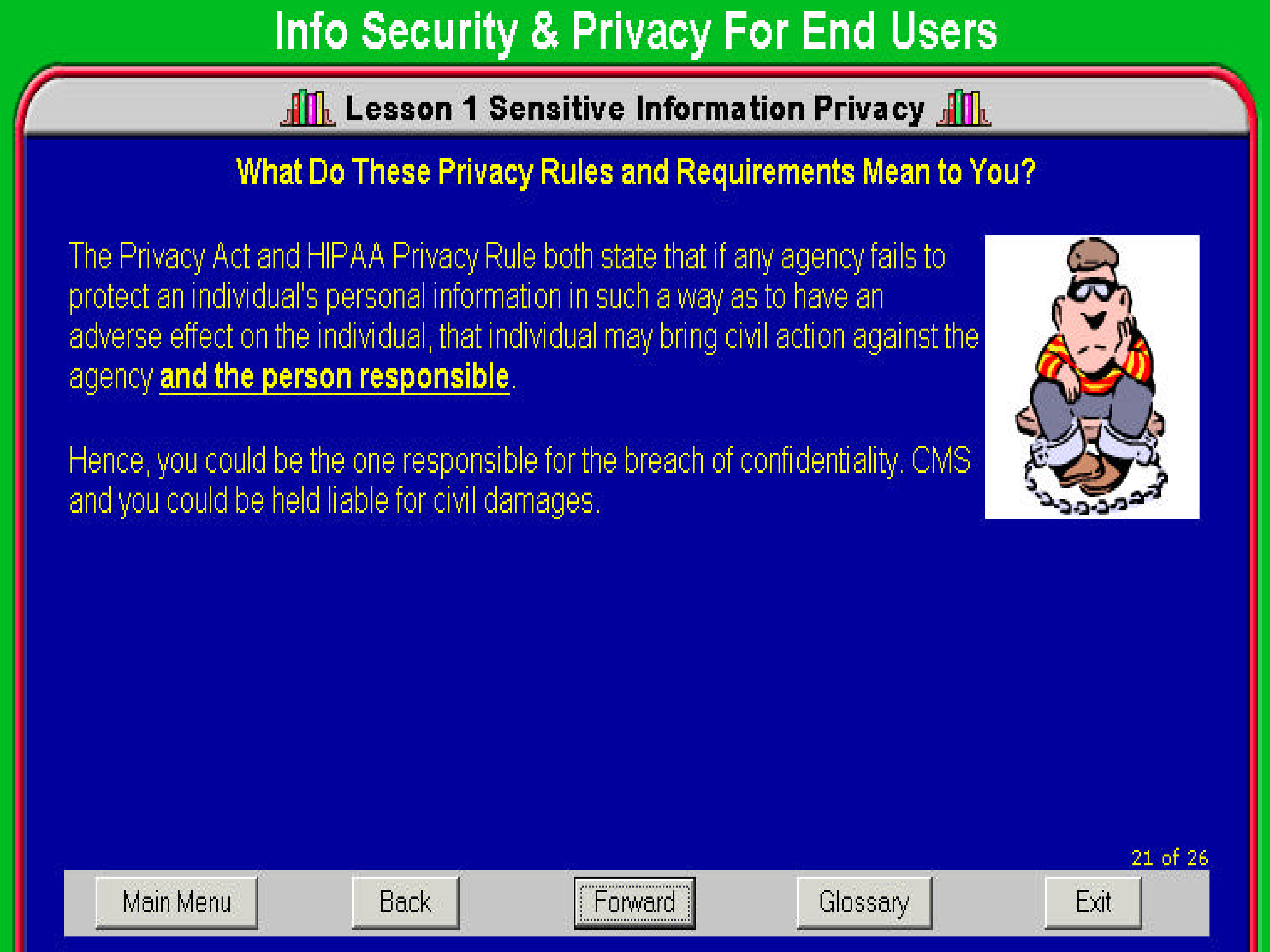
HELP! HELP! HELP! – I think I have a VIRUS…

"That is – my computer has a virus. Well I think it does, but I'm not sure. I received an e-mail from a friend of a friend's sister who said that if a computer boots up on the first try then you should assume you have a virus and delete all of your files in order to stop the virus from spreading."

Information Security & Privacy

End-User Computer Based Training (CBT)

- Web based
  - Currently intranet
  - On/about May 2003 – internet (www.CMS.hhs.gov/it/security)
- CMS employees – mandatory completion by December 31, 2002
- On/about May 2003, mandatory for CMS Userid annual recertification



Info Security & Privacy For End Users

Lesson 1 Sensitive Information Privacy

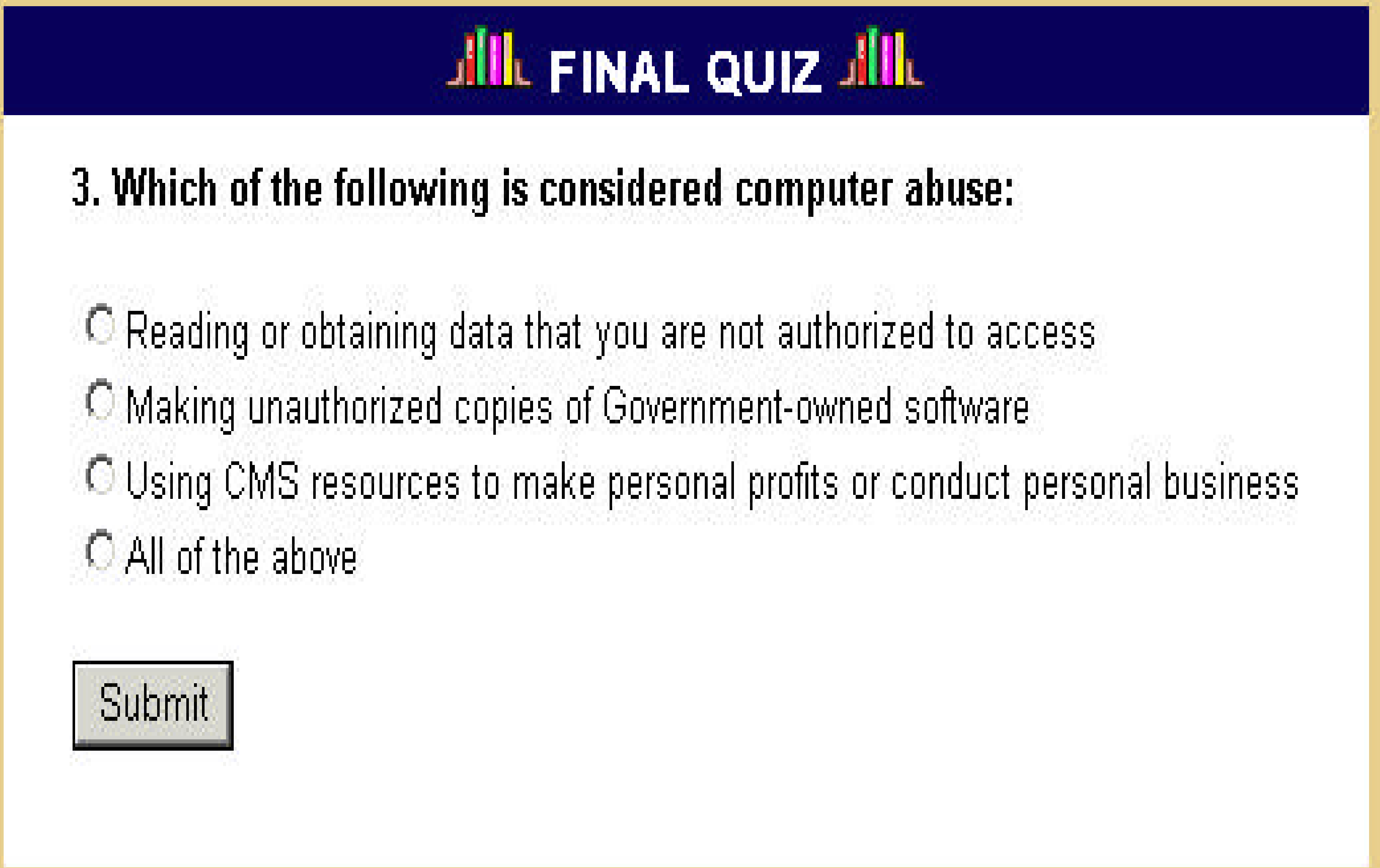
What Do These Privacy Rules and Requirements Mean to You?

The Privacy Act and HIPAA Privacy Rule both state that if any agency fails to protect an individual's personal information in such a way as to have an adverse effect on the individual, that individual may bring civil action against the agency **and the person responsible**.

Hence, you could be the one responsible for the breach of confidentiality. CMS and you could be held liable for civil damages.

21 of 26

Info Security & Privacy For End Users



FINAL QUIZ

3. Which of the following is considered computer abuse:

○ Reading or obtaining data that you are not authorized to access

○ Making unauthorized copies of Government-owned software

○ Using CMS resources to make personal profits or conduct personal business

○ All of the above

Getting Started – Lessons Learned

- Follow NIST SP 800-50, Building an IT Security Training & Awareness Program instead of producing:
  - Current Awareness & Training Report
  - Awareness & Training Structure Report
  - Framework Report
  - Program Details

- Immediately begin work on:
  - Senior Executive briefing
  - End-User training
  - Managers briefing
  - ISSO course

Program - Lessons Learned

- Different target audiences with different needs
- Wanted a "perfect" CBT
- Start early with end user "reminders"
- Be prepared with answers, resources and tools

Best Practices

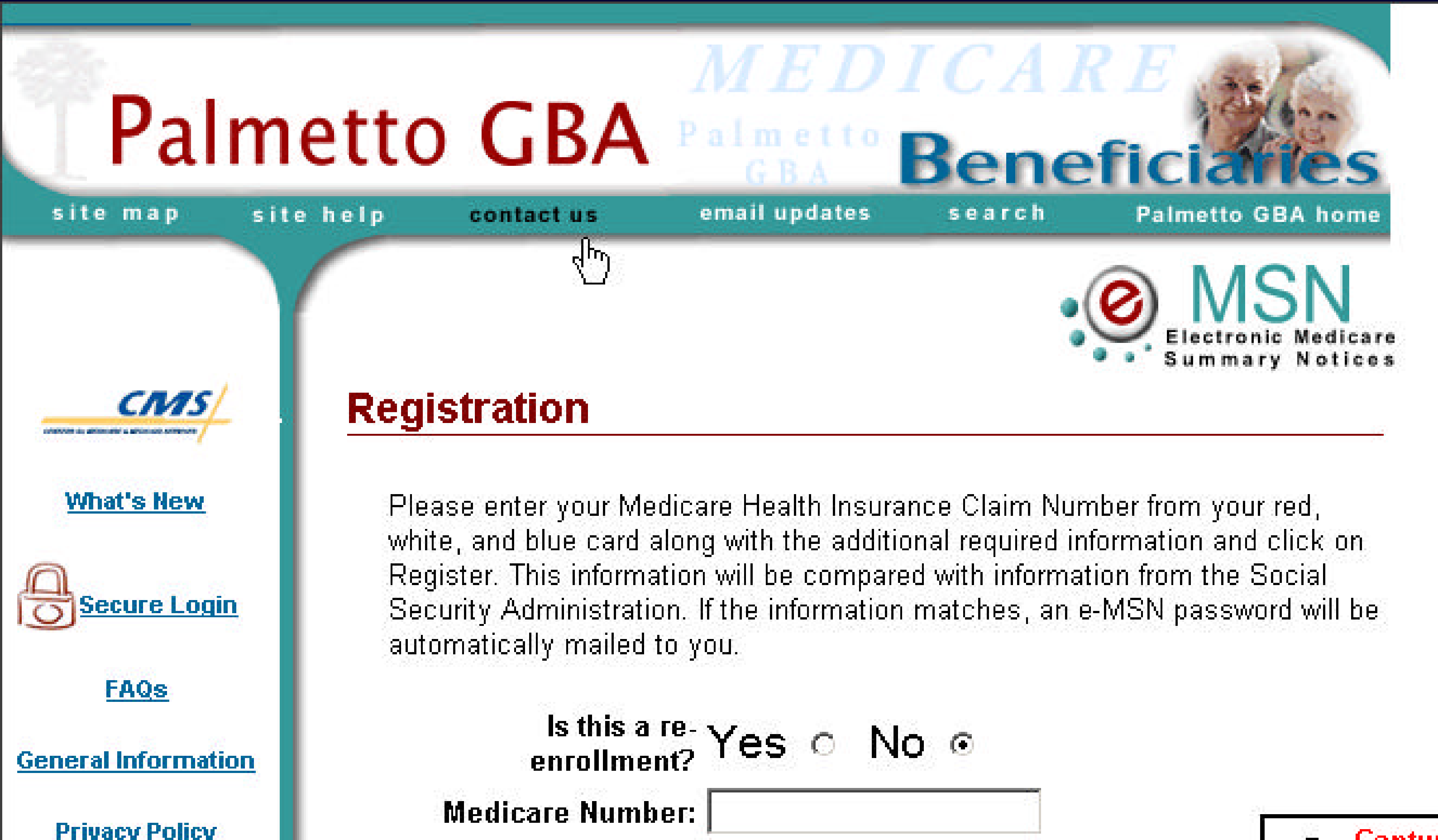
- Partner with Privacy Officer / Advocates
- End-user Awareness
  - Technology-based (web, CD’s etc.)
  - Awareness Days/Conferences/Trinkets
  - Paper-based (newsletter, tri-fold)
  - CyberTyger E-mail
- Management Awareness - especially for system development areas
- Technical Training - Developers/ Administrators/ISSOs
- Intranet Web Site

What’s Next

- e-Gov Initiatives
- Modernization
- Expanded audience

Centers for Medicare & Medicaid Services (CMS)

E-Gov Initiatives



Palmetto GBA

Registration

Please enter your Medicare Health Insurance Claim Number from your red, white, and blue card along with the additional required information and click on Register. This information will be compared with information from the Social Security Administration. If the information matches, an e-MSN password will be automatically mailed to you.

Is this a re-enrollment? Yes ○ No ●

Medicare Number:

Thank You !!!

- CyberTyger@cms.hhs.gov
- www.cms.hhs.gov/it/security

Julie Boughn

Director, CMS-OIS-SSG-DCES

Jboughn@cms.hhs.gov

Sharon Kavanagh

Training & Awareness Coordinator

Skavanagh@cms.hhs.gov