Joint STATE-USAID Solution

Information Systems Security

Line of Business

March 7, 2007

Current Events Highlight Challenge

Management Responses Needed

From: **CIOs and Deputy CIOs [mailto:CIO-DEPTCIO@LISTSERV.GSA.GOV]** On Behalf Of **Evans, Karen**
Sent: **Wednesday, June 07, 2006 5:05 PM**
To: **CIO-DEPTCIO@LISTSERV.GSA.GOV**
Subject: **[CIOCD] Request for Information**
Importance: **High**

Hi Everyone

By 8:00am tomorrow morning, I need to have a status of where you are on the requirement included in the May 22, 2006 memo from Clay which states:

"In addition, please ensure your agency employees are reminded within the next 30 days of their specific responsibilities for safeguarding personally identifiable information, the rules for acquiring and using such information as well as the penalties for violating these rules.“

Please report the percentage of employees notified and the method of notification.

Thanks in advance
Karen

Response Provided

From: **Streufert, John(M/DCIO))**
Sent: **Thursday, June 08, 2006 8:40 AM**
To: **'Evans, Karen'; Karen_Evans@omb.eop.gov; 'Schlarman, Glenn R.'**
Cc: **Bussow, Mark; Heneghan, Phil(M/DCIO); Moore, George(M/DCIO); Hughes, Mike(M/AA:AINS); Alumbaugh, John(GC/LE); Haiman, Arnold J(GC)**
Subject: **RE: [CIOCD] Request for Information**
Importance: **High**

Karen,

Summary. Within 24 hours after Clay Johnson's notice **(May 23, 2006)** USAID had notified its staff **[in 20 time zones] world-wide regarding employee responsibilities for protecting personally identifying information as a result of the … incident. This event included confirmed receipt of delivery to individuals by name at 80 overseas locations, awareness training and testing of concept understanding.**

…

- **97.7% coverage (8,268 people)**
- **All Agency employees who failed to answer the True –False question concerning the … incident correctly the first time were immediately retested.**
- **Fifty-five employees world-wide answered the question incorrectly twice**
- **And 169 personnel did not respond to the test.**

JSAS Meets These Needs

- New threats need quick response – and confirmation that the threat was understood
- Adults learn by doing – daily security interactions build habits and reinforce learning
- Users need – comprehensive training and periodic refreshment, remediation for transgressors

Agencies Selecting JSAS Receive

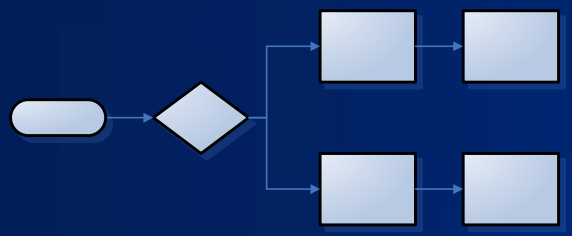
- ✓ A comprehensive approach to IT Security Awareness training consistent with NIST SP 800-50
- ✓ A proven, reliable solution that verifies retention of material and concepts
- ✓ A two-part solution -- current daily training and periodic in-depth training
- ✓ A well established training program that uses industry standard web-based delivery mechanisms and secure back-end database technology

Leverage E-Training Provider

- **The Foreign Service Institute**
  - An OPM-authorized Service Provider
  - Decades of experience training other federal agencies
  - Reliable reimbursement processes under the Economy Act
  - Special contracting and hiring authorities under the Foreign Service Act which provide great flexibility
- **This customer-driven, service-oriented delivery highlights the quality and experience of the JSAS**

JSAS Offers Leading

People



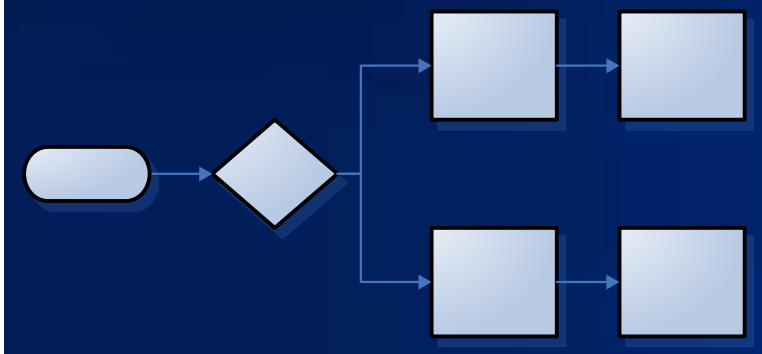
Processes

Technology

People

- **Security Subject Matter Experts**
  - Certified Security Practitioners
  - Threat Specialists
  - Policy Analysts
- **Instructional Systems Designers**
  - Specialists in Adult Learning
- **Data Managers**
  - Slicing and Dicing Data Supporting Metrics

Processes



- **JSAS Elements**
  - Awareness Needs Assessment
  - Customer Relationship Management
  - Content Management
  - Technology Management
  - Risk Management
  - Rapid Response
  - Metrics – Effectiveness & Efficiency
  - Training Administration

Technology

- **JSAS is**
  - Easy To Use
  - Comprehensive and Complete
  - Timely, Compliant and Secure
  - Flexible in Delivery
    - Annual Training
    - Daily Refresher

The JSAS Awareness Package

- **Adults Learn By Doing (Effective)**
  - Comprehensive Awareness Course
  - Awareness Daily Reminder
  - Required Interaction
- **Results (Efficient)**
  - Instant Feedback
  - Certificate of Completion
  - Automated Administration

Tips of the Day

Daily Refresher Training Tool

Security Tips of the Day

Deliver awareness.

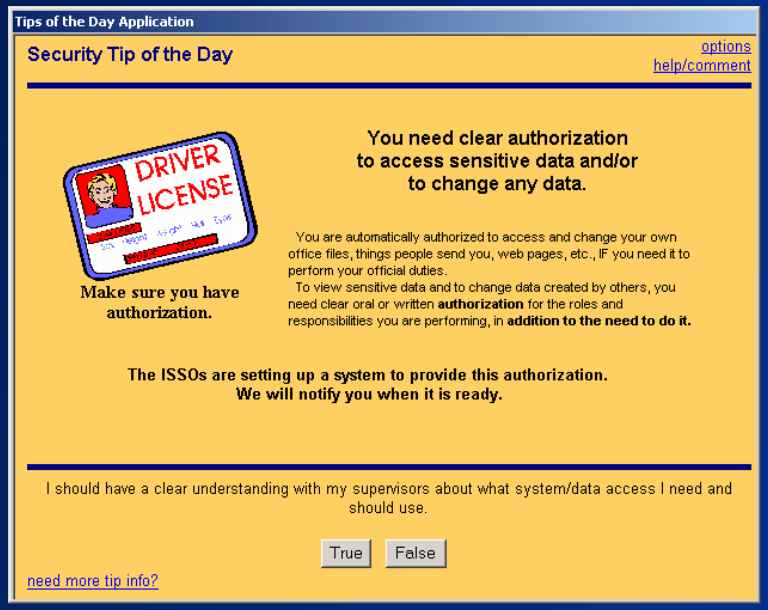
Protect information.

Normal Operation

- User logs into system and receives a tip

- User reads the question
- User presses one button to answer

Normal Operation



- No user navigation is required
- Login is an automatic result of network login
- Current frequency: 1 tip per workday
- Concise and Actionable
- New users are automatically registered
- Login, tip, and response are all logged in the Database

User Report

User May Click to Review Tip

Security Tips of the Day - Grade Summary Report: - Microsoft Internet Explorer provided by USAID

USAID FROM THE AMERICAN PEOPLE

Security Tips of the Day - Grade Summary Report:

From: 8/27/2006 To: 9/26/2006 Go

Prepared For: THUSAID\CKeever on Tuesday September 26, 2006

Your Overall Score: 88%

0% 20% 40% 60% 80% 100%

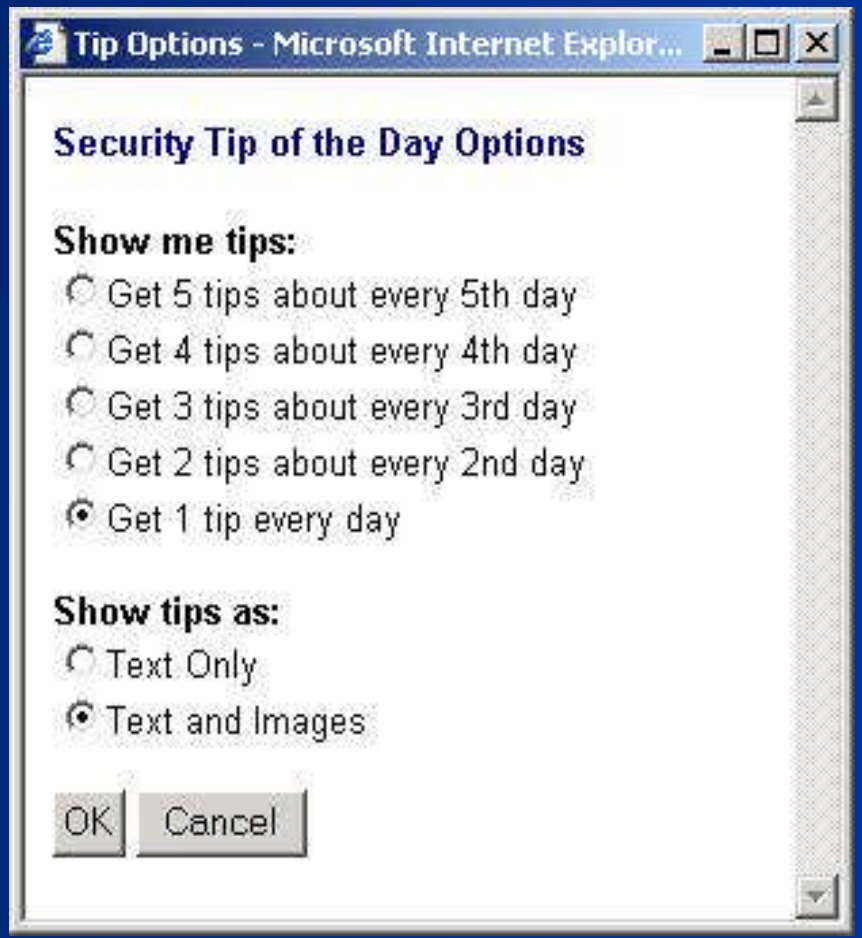
te	Question	Correct Answer	Your Answer	
006	Press OK to continue.	OK	OK	
09/26/2006	Medical information is not considered SBU.	False	True	✗
09/26/2006	I am authorized to configure my anti-virus and security settings however I think works best.	False	False	✓
09/26/2006	Data stored in a network data space is not backed up.	False	False	✓
09/26/2006	If I connect my laptop to non-USAID networks, it is more likely to become infected with viruses.	True	True	✓
09/25/2006	I should have a clear understanding with my supervisors about what system/data access I need and should use.	True	True	✓
09/22/2006	I should only use approved software.	True	True	✓
09/22/2006	I can process classified information on any computer in USAID.	False	False	✓
09/22/2006	If I know there is improperly installed software, I should still use it.	False	False	✓
09/22/2006	Press OK to continue.	OK	OK	

10 Results Per Page Results displayed: 1 - 10 of 41 << < Page: 1 of 5 > >>

Total Tips Given: 29 Answered: 100% Scored: 26 Correct: 88%

Customization

- **User Options:**
  - Reached from the options link on any tip
  - User may choose to get more tips less often
  - For 508 compliance, user may request text only tips which are black & white



Custom Frequency

- **Users have system-roles**
- **System-roles contain content categories**
- **Categories contain tips**
- **Customer agencies have great flexibility in dialing in tip frequency by role, category, and or individual tips, to fine tune content to emerging issues/threats**

Categories of Tips

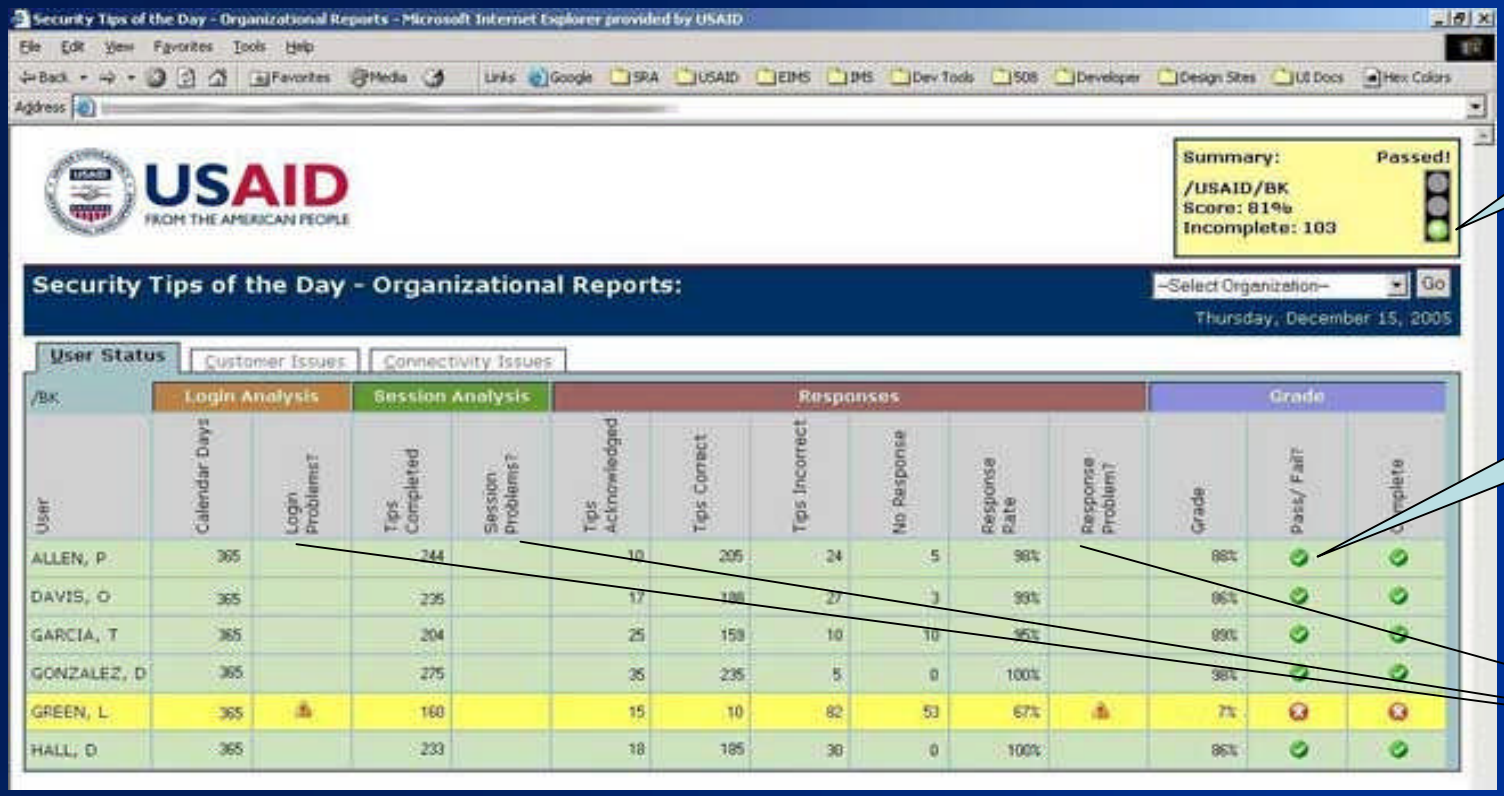
	NIST 800-53 Categories	Tier I General	Tier II Special
AC	Access Control	X	X
AT	Security Awareness and Training		X
AU	Audit and Accountability		X
CA	Certification, Accreditation, and Security Assessment		X
CM	Configuration Management	X	X
CP	Contingency Planning	X	X
IA	Identification and Authentication	X	X
IR	Incident Response	X	X
MA	System Maintenance	X	X
MP	Media Protection	X	X
PE	Physical and Environmental Protection	X	X
PL	Security Planning		X
PS	Personnel Security	X	X
RA	Risk Assessment		X
SA	System and Services Acquisition		X
SC	System and Communications Protection	X	X
SI	System and Information Integrity	X	X

Agency Specific Tip Topics

Access Management
Data Protection
Emergency Preparedness
Ethics
Handling SBU
Intellectual Property Mgmt
Introductory Tips (Tips on Tips)
Network Access
Password Protection
Password Selection
Personal Computers

Physical Property Mgmt
Privacy
Processing Classified
Prohibited and Inappropriate Behavior
Reducing Phone Call Costs
Security Incidents
Software Management
Spyware, Adware, Malware
Virus Protection
Workstation Protection

Organizational Metrics



Organization's Score

Individual's Score

Diagnostic Symptoms

Configuration

Manage TOD Data - Microsoft Internet Explorer provided by USAID

File Edit View Favorites Tools Help

Back Search Favorites Media

Address http://2k3efxwshnd02.us.usaid.gov:7777/portal/page?_pageid=53,22344,53_2 Go Links SnagIt

Security Tips of the Day

Deliver awareness. Protect information.

Home Help

Customize Account Info Logout

Alerts | Tips | Organizations | Users | Meta-Data

Defaults | Assign an Alert to a Group | Reports

This tab allows you to control the default alerts that will given to new users.

Default are normally used to train new users in how to use the Tips of the Day. The tips you list here will be given to new users, once per day, BEFORE any normal tips are given to them. They are given in order of priority. (Lower numbers indicate higher priority.)

New User Default Alerts List — Customize

Id	Tip Id	Priority	Urgent Flag	Date Created	Date Last Modified
5	50	1	F	26-SEP-06	(null)
6	107	2	F	26-SEP-06	(null)

New User Default Alerts Form — Customize

Inserted one record.

Insert Query Reset

Tip

Priority

Urgent Flag False

Insert Query Reset

Area Reserved for common footer across all tabs.

Done Local intranet

Search Dialog - Microsoft Internet Explorer provided by ...

Enter search criterion. (Example: a% will find all values begining with "a"). Searches are case insensitive.

%SBU% Find... Close

U-SBU-T-01-TRUE-01
U-SBU-T-02-FALSE-01
U-SBU-T-02-FALSE-02
U-SBU-T-02-TRUE-01
U-SBU-T-03-FALSE-01
U-SBU-T-03-FALSE-02
U-SBU-T-03-TRUE-01
U-SBU-T-04-TRUE
U-SBU-T-05-FALSE
U-SBU-T-05-TRUE

Row(s) 1 - 10

Next

Configuration

These Configurable Features, and More

- Systems Covered
- System Roles Covered
- The probability of selecting content from a System Role
- Categories of content within each System Role
- The probability of selecting a category within the selected system role.
- Tips within each category
- The probability of selecting a tip from within a category
- New User Defaults
- New User Default Alerts
- Customer Organizational Structure
- Customer Organizations
- Organizational Contact Types
- Contact Address Types
- User-Account Types (active, inactive, group, etc.)
- User Roles for Administration and Reporting
- Method of linking users to organization (via domain or directly)
- Questions for each set of tip-content.
- Buttons that are used for answers
- Buttons for each tip-content/question combination
- Whether to record user IP address
- Whether to record user machine name
- Whether to record user MAC address
- Passing Grades, etc.

Technically Standard & Scalable

Model Area	Components
Access Channels	User – IE Web Browser HTML V3
Delivery Channels	Application integration and access via standard IE
Service Transport	HTTP or HTTPS (SSL); SMTP for user feedback and error logging
Database Storage	SQL-Server and/or Oracle 10g
Delivery Servers	IIS and Oracle Application Server; Windows Platforms
Hardware/Infrastructure	Mature configurations designed to promote security which are regularly scanned for vulnerabilities (then graded and remediate)
SW Engineering	Mature processes with ample testing, configuration management
SW Architectures	Mature simple industry standard platform architectures
Business Logic	The business logic layer is maintained in the software between the database and the presentation layers
Data Interchange	Data interchange between the presentation layer and the database is managed by structured software between the business model and the database
Data Administration	The data model is well normalized and uses standard naming conventions
Presentation/ Interface	The presentation layer is provided via Internet Explorer. Standard methods are used to generate the HTML pages: these include ASP and JSP pages
Integration	Downloads to standard tools (such as Excel) using COTS components
Interoperability	Proposed SOA will provide this capability, as needed

Security Compliance

Factor	Summary
Privacy	PII where employed is fully protected
Authentication	Authentication is role based
Confidential	Various users and admin role have different access
Integrity	Only the executable code has the ability to write results. Results are not modifiable
Available	Solution has a high availability rate (>95%)

CyberSecurity Awareness Course

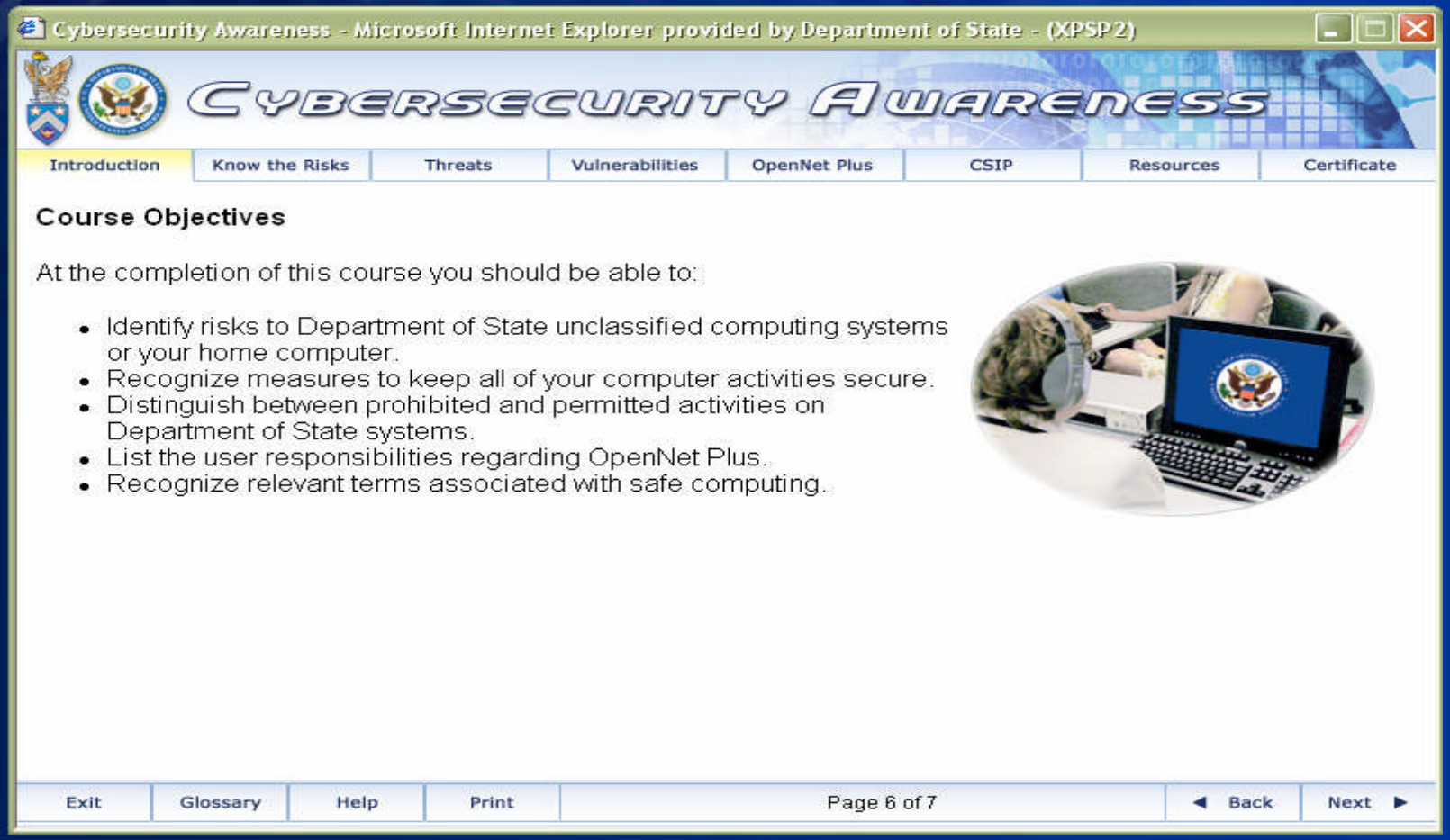
The Course

CyberSecurity Awareness is a 30-minute web-based course requiring only an IE browser.

Context

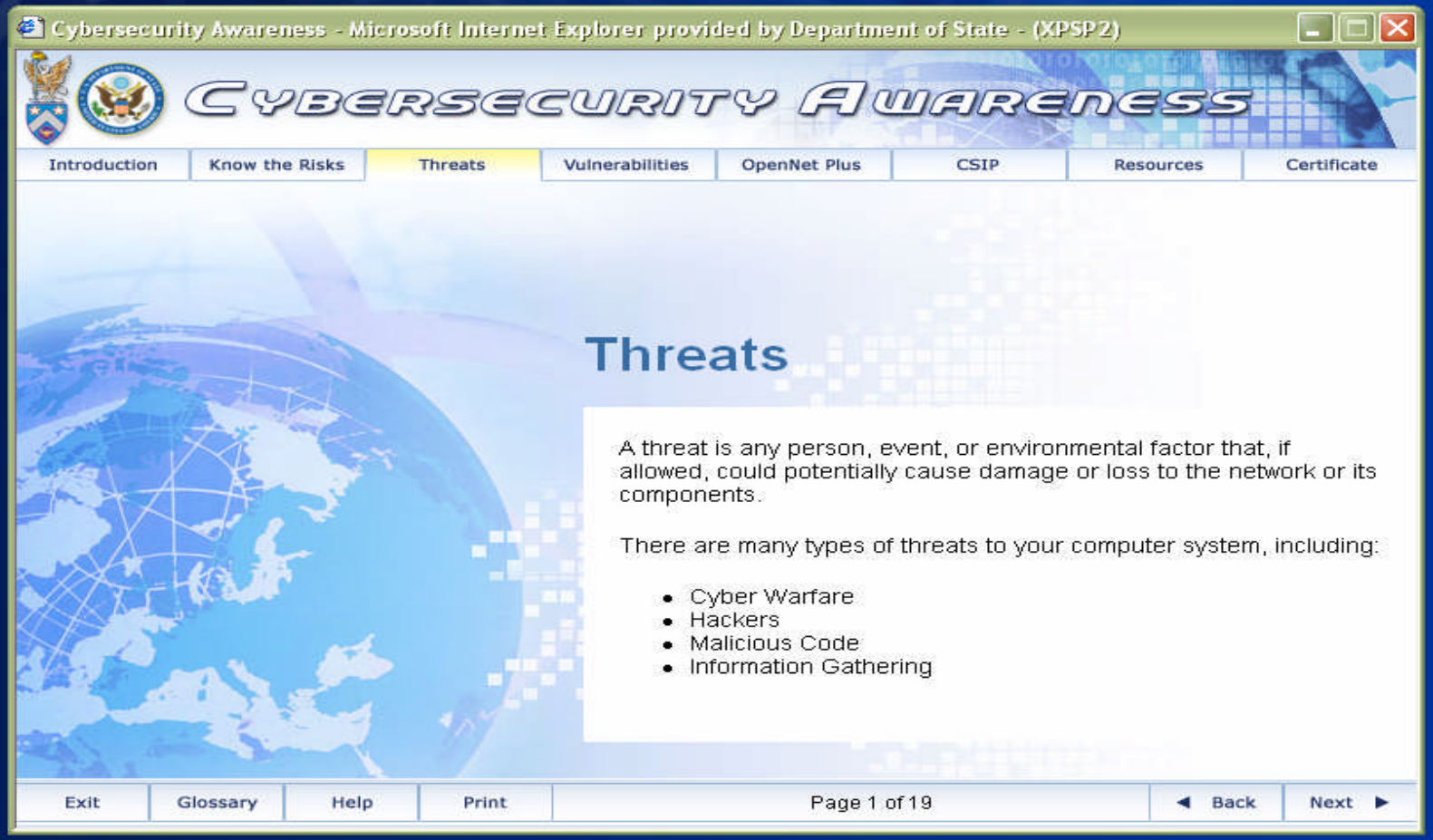
Purpose and context are clearly stated.

Purpose



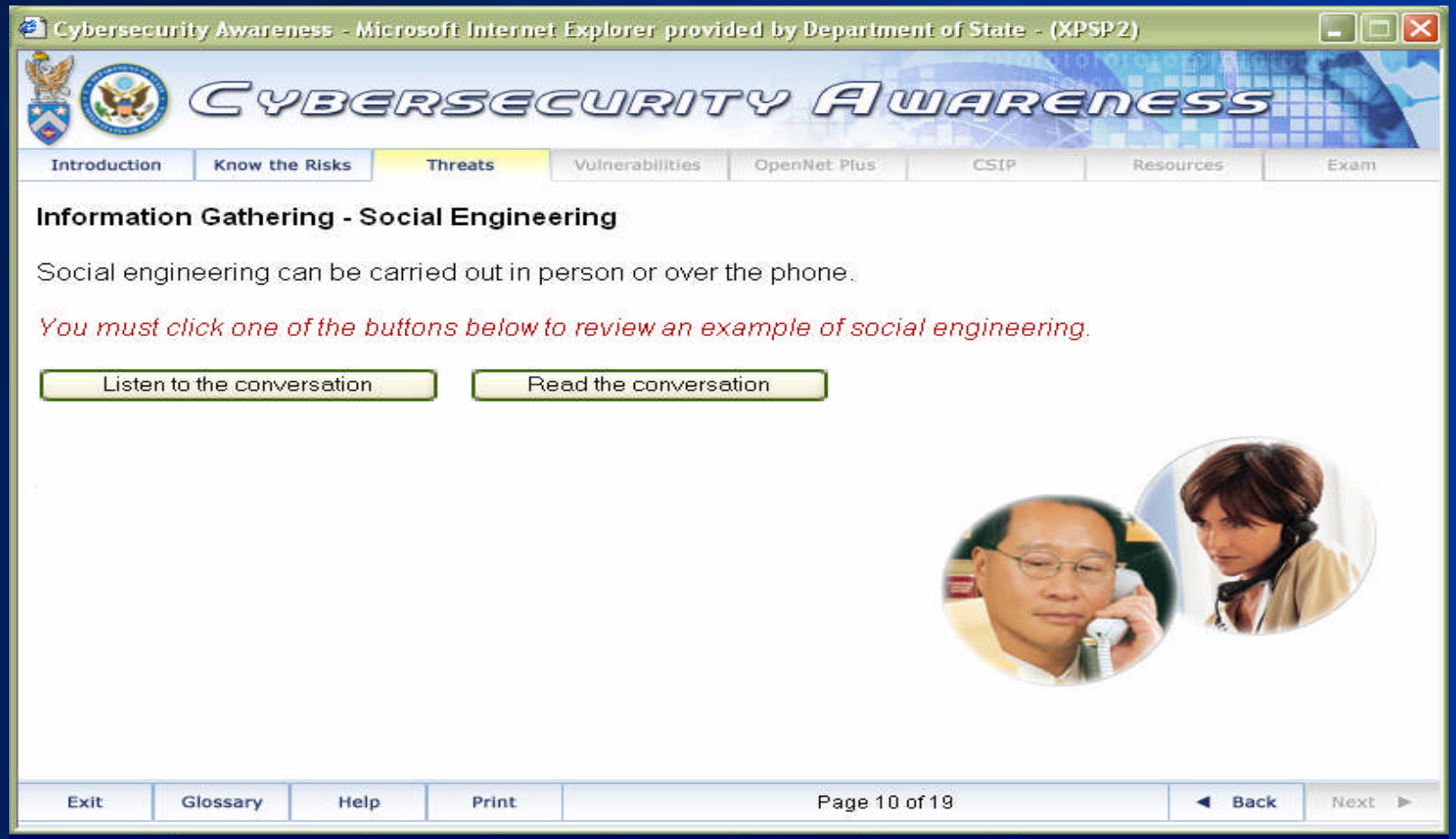
Course objectives are clearly stated.

Content



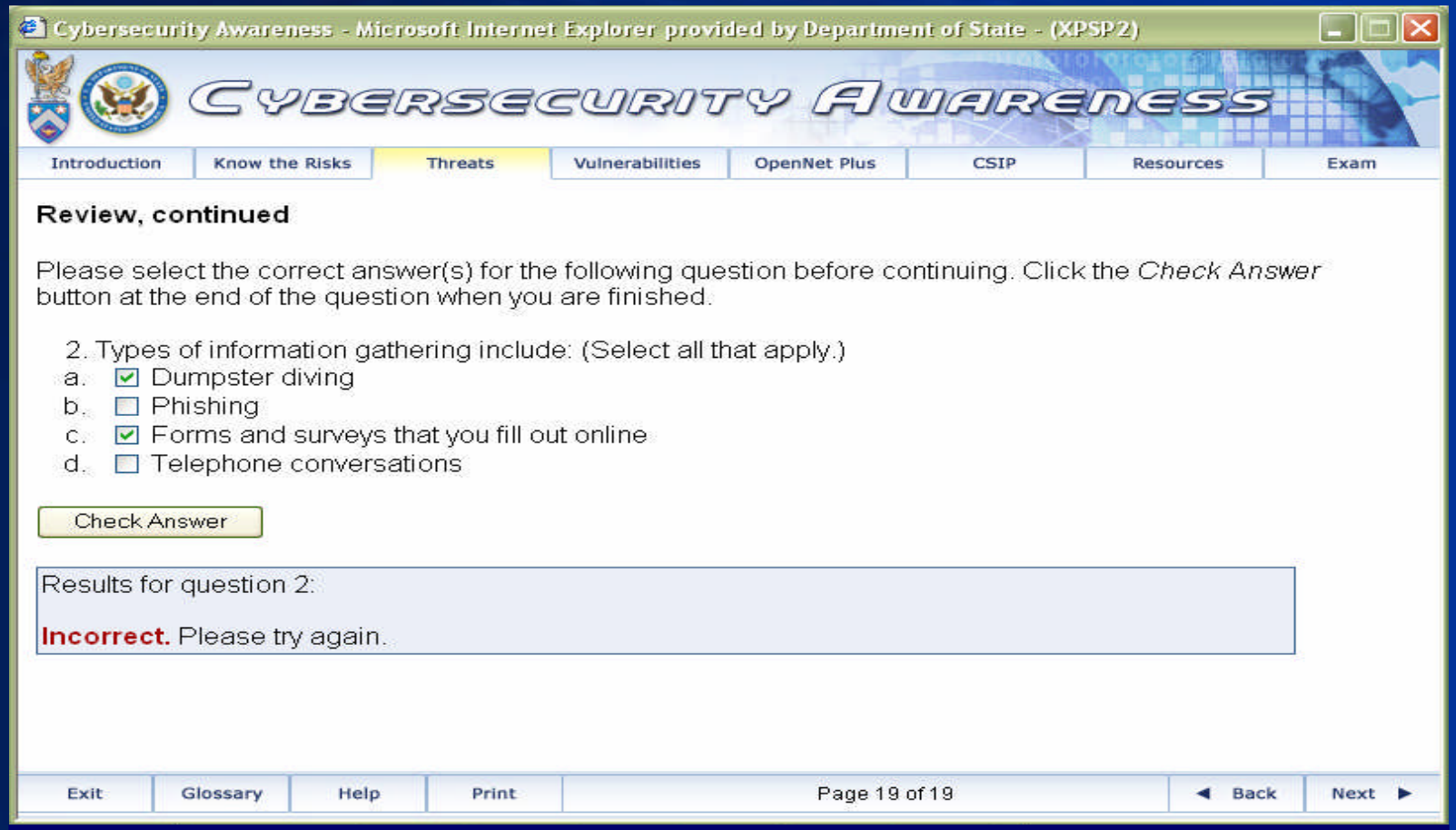
Content reflects NIST 800-50 Guidance.

Interaction



A variety of interactive features improve learning. This is an audio example of social engineering.

User Action and Response



The end of each section includes an interactive quiz. Immediate feedback is provided on the choices made.

User Action and Response

Cybersecurity Awareness - Microsoft Internet Explorer provided by Department of State - (XPSP2)

CYBERSECURITY AWARENESS

Introduction | Know the Risks | Threats | Vulnerabilities | OpenNet Plus | CSIP | Resources | Exam

Review

Please select the correct answer for each of the following questions before continuing.

1. Select the BEST password.
a. 1qazxsw2
b. Colorado64
c. !G0b0s0x!
d. george

Results for question 1:

Correct. c is the correct answer.

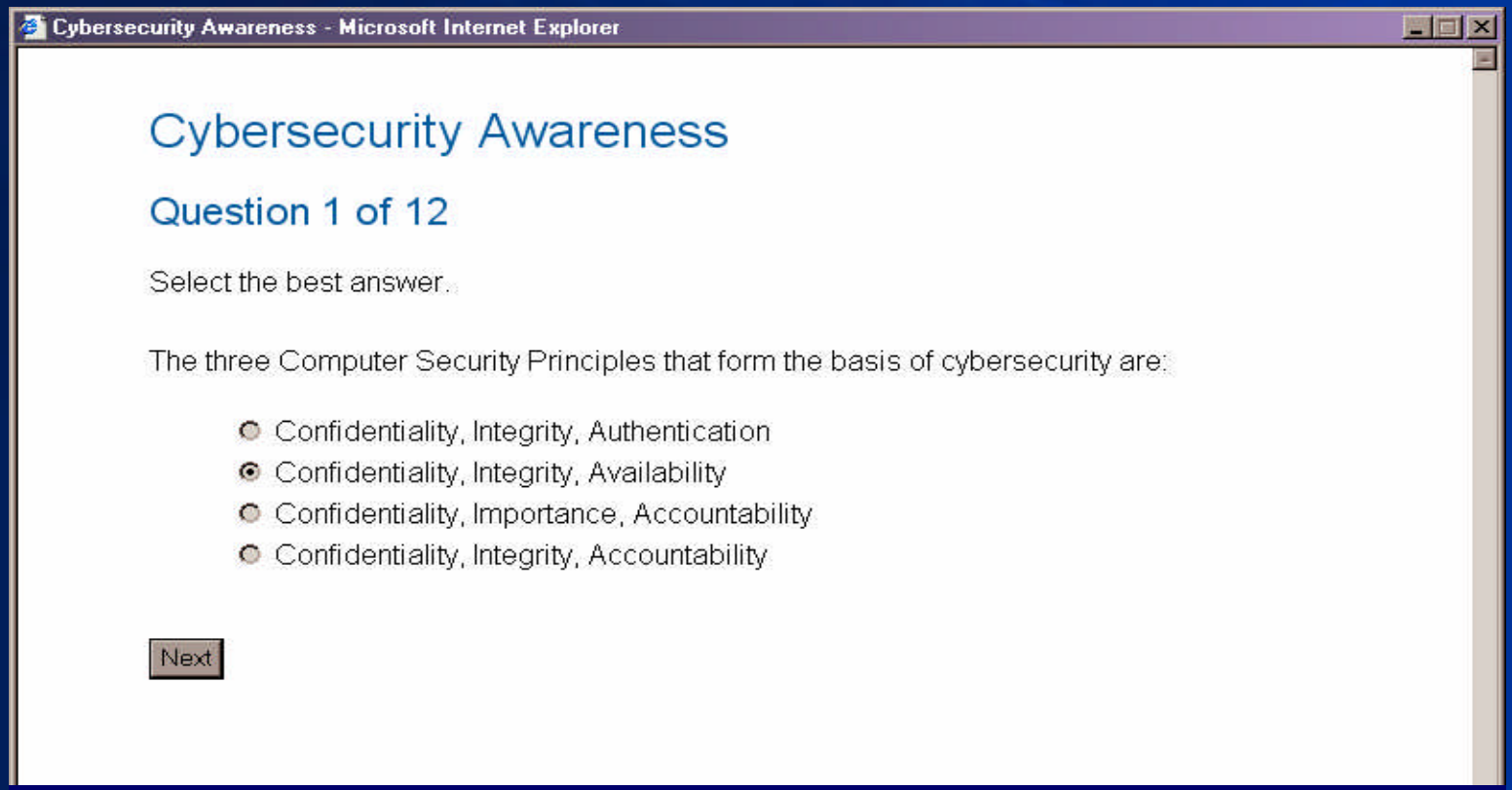
This password uses all 4 character types in a creative and unusual way. This **is** the best password of the available options.

2. You should not open e-mails unless they are from a STATE.GOV address.
a. True
b. False

Exit | Glossary | Help | Print | Page 12 of 13 | ◄ Back | Next ►

When the answer is correct, there is additional positive reinforcement.

Exam



Exam consists of 12 questions of different types (multiple choice, multiple answer, true/false) randomly selected from a pool covering topic areas.

Exam Results

Cybersecurity Awareness - Microsoft Internet Explorer

Close Window

Cybersecurity Awareness

Exam

Congratulations, you passed the exam. You answered 10 out of 12 questions correctly.

View and print your completion certificate

You will be able to access the course material and reprint your certificate for up to one year.

Your certificate will open in a new browser window for you to print it. The certificate is designed to print in portrait orientation. You may need to adjust your printer settings accordingly.

You may print a copy of your completion certificate for your records. Please notify your ISSO that you have completed the course and passed the exam.

Participate in a course evaluation survey

The questions you answered incorrectly are listed below.

Missed Questions

Which of the following is allowed on OpenNet Plus? (Select all that apply.)

a. Sending personal e-mail
b. Fundraising
c. Personal Web-browsing
d. None of the above

At the end, users get immediate feedback on which questions they got wrong – but not why. They can go back to any section and review the material.

User Certificate

- **Completion certificate is immediately available to print or e-mail**

- **The user can access it again anytime during the following year**

George P. Shultz
National Foreign Affairs Training Center
Foreign Service Institute
U.S. Department of State

This certificate is awarded to

Beta Tester

In recognition of successful completion of
PS800: Cybersecurity Awareness

February 27, 2007

This certificate is valid until February 27, 2008.

Note: The dates are based on Eastern Standard Time (EST).

Survey

Cybersecurity Awareness: Survey - Microsoft Internet Explorer

Cybersecurity Awareness

Course Evaluation Survey

Instructions
Please choose your response to the items. Rate aspects of the course on a 1 to 5 scale - 1 equals "strongly disagree" and 5 equals "strongly agree." Your feedback is anonymous and is sincerely appreciated. Thank you.

1=Strongly disagree, 2=Disagree, 3=Neutral, 4=Agree, 5=Strongly agree

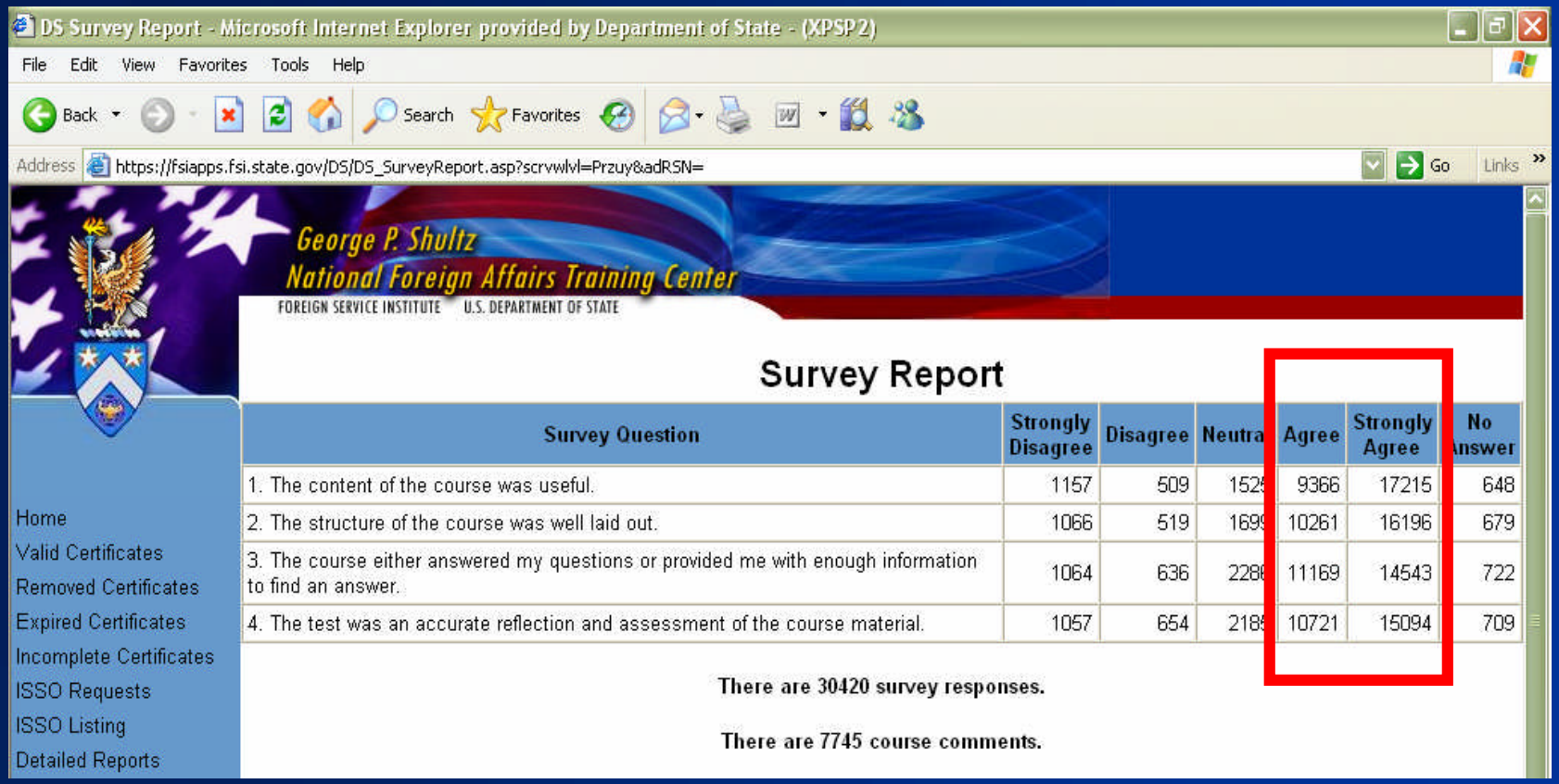
Review Items	Comments
1. The course navigation is easy to follow.	1 2 3 4 5
2. The content is clear and readily understood.	1 2 3 4 5
3. The course either answered my questions or provided me with enough information to find an answer.	1 2 3 4 5
4. The exam was an accurate reflection and assessment of the course material.	1 2 3 4 5

5. Do you have any comments or suggestions?

Submit Evaluation

More than 30,000 surveys have been completed.

Survey Reporting



Survey Question	Strongly Disagree	Disagree	Neutra	Agree	Strongly Agree	No Answer
1. The content of the course was useful.	1157	509	152	9366	17215	648
2. The structure of the course was well laid out.	1066	519	169	10261	16196	679
3. The course either answered my questions or provided me with enough information to find an answer.	1064	636	228	11169	14543	722
4. The test was an accurate reflection and assessment of the course material.	1057	654	218	10721	15094	709

All stakeholders can have access to the results of the user survey.

Reporting

- **Periodic reports on**
  - Successful completions
  - Overdue re-takes
- **Ad hoc inquiry capability**

Benefits

The course meets several needs

- **Initial training for new users**
- **Annual refresher training**
- **Remediation training for miscreants**

Business Operations

Administration

The Foreign Service Institute provides financial and acquisition administration

- Legal authorities
- Decades of interagency financial dealings
- Customers from 47 agencies/services
- An OPM-authorized e-Training Service Provider under the Human Resources Line of Business

Business Options

- **Basic Services**
  - Re-branding
  - Help Desk M-F 8am-5pm Eastern Time
  - Content Refreshment
  - Reporting
- **Hosting**
  - Customer Hosts
  - JSAS Hosts
- **Premium Services**
  - Content Additions
  - Customization
    - Ad hoc reporting
    - Technology
    - Look and feel
  - 24x7 Help Desk

Planning Documents

- Service Level Agreements
- Customer Profile
- Migration Plan
- eMail Questions to JSAS@State.Gov
- Web Page http://JSAS.state.gov

Customer Cost

- **Assumptions**
  - An agency of 100,000 users
  - JSAS hosts the solution
  - No changes to content except branding
  - No changes to roles and responsibilities
- **Base planning figure**
  - Tip of the Day $3/user/year
  - CyberSecurity Course $1/user/year
- **Customer requirements will affect price**

Customer Cost

Customer requirements will affect price

- Number of users
- Operating systems
- Firewalls
- Browsers
- Customer-hosting
- Content additions/deletions/alterations
- Any other agency specific or unique requirement
- Adjustments to roles and responsibilities

Conclusion

Agencies Selecting JSAS Receive

- ✓ A comprehensive approach to IT Security Awareness training consistent with NIST SP 800-50
- ✓ A proven, reliable solution that verifies retention of material and concepts
- ✓ A two-part solution -- current daily training and periodic in-depth training
- ✓ A well established training program that uses industry standard web-based delivery mechanisms and secure back-end database technology

Joint STATE-USAID Solution

Complimentary Products, Comprehensive Solution