ISSLOB SSC CYBERSECURITY AWARENESS

U.S. DEPARTMENT OF STATE

JSAS Cyber Security

- IT Security Awareness training consistent with NIST SP 800-50
- A proven, reliable solution that verifies retention of material and concepts
- A well established training program that uses industry standard web-based delivery mechanisms and secure back-end database technology

What’s New

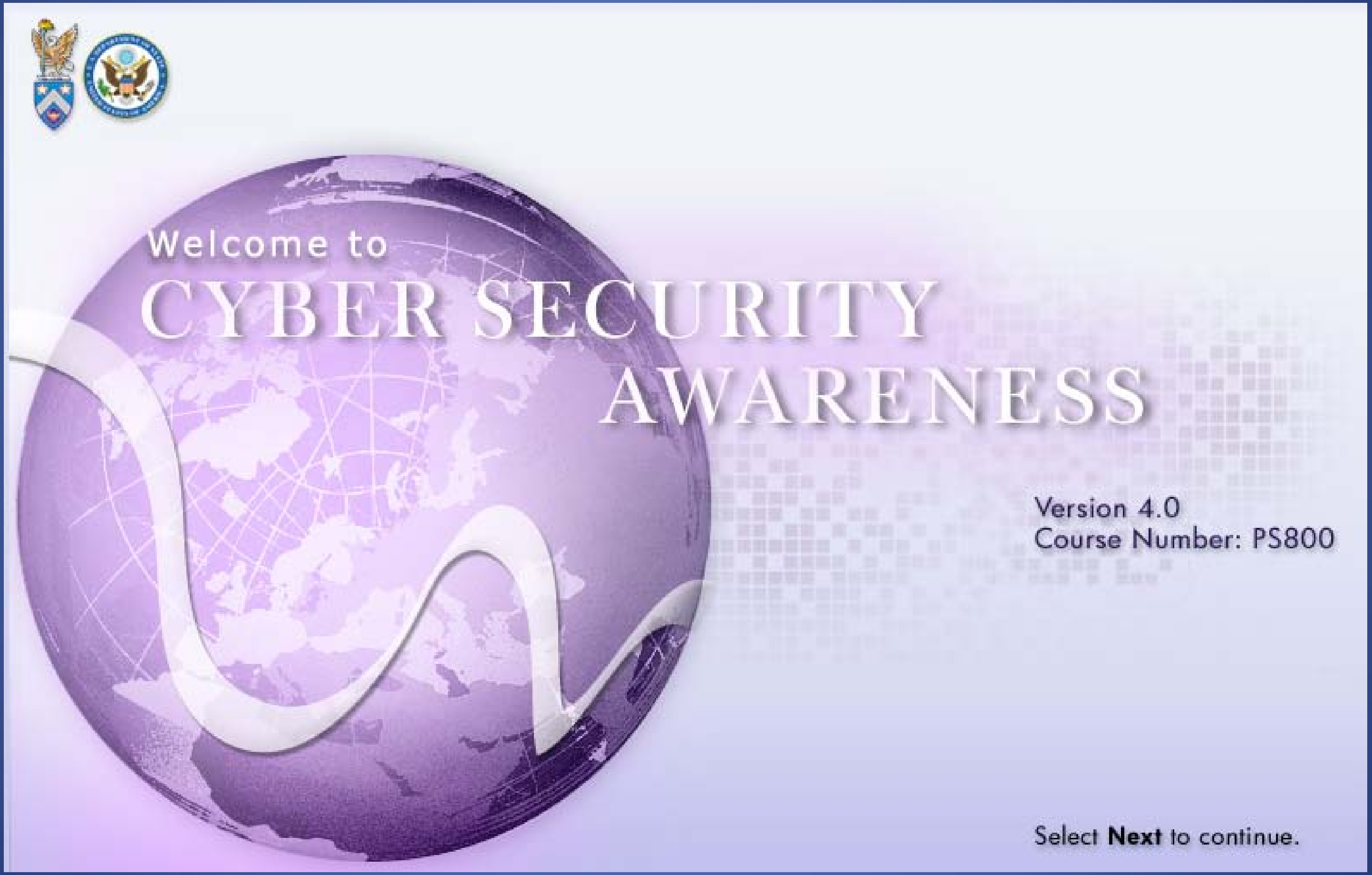
- Increased user base and LMS implementations
- New look & feel: Completely re-written for fresh approach
- New technologies such as mobile computing and social networking addressed in greater detail
- Review questions based in real-world situations that ask the learner to apply their knowledge
- Additional test questions (over 150 in pool)

Total JSAS CSA Users By Agency

Agency	Users
USHMM	719
CSOSA	≈ 1,500
NLRB	1,690
AO US Courts	1,723
FTC	1,729

Agency	Users
Peace Corps	2,677
NARA	4,353
USCIS	4,944
EPA	23,558
State	82,540
TOTAL	**≈125,433**

The Course



Welcome to

CYBER SECURITY AWARENESS

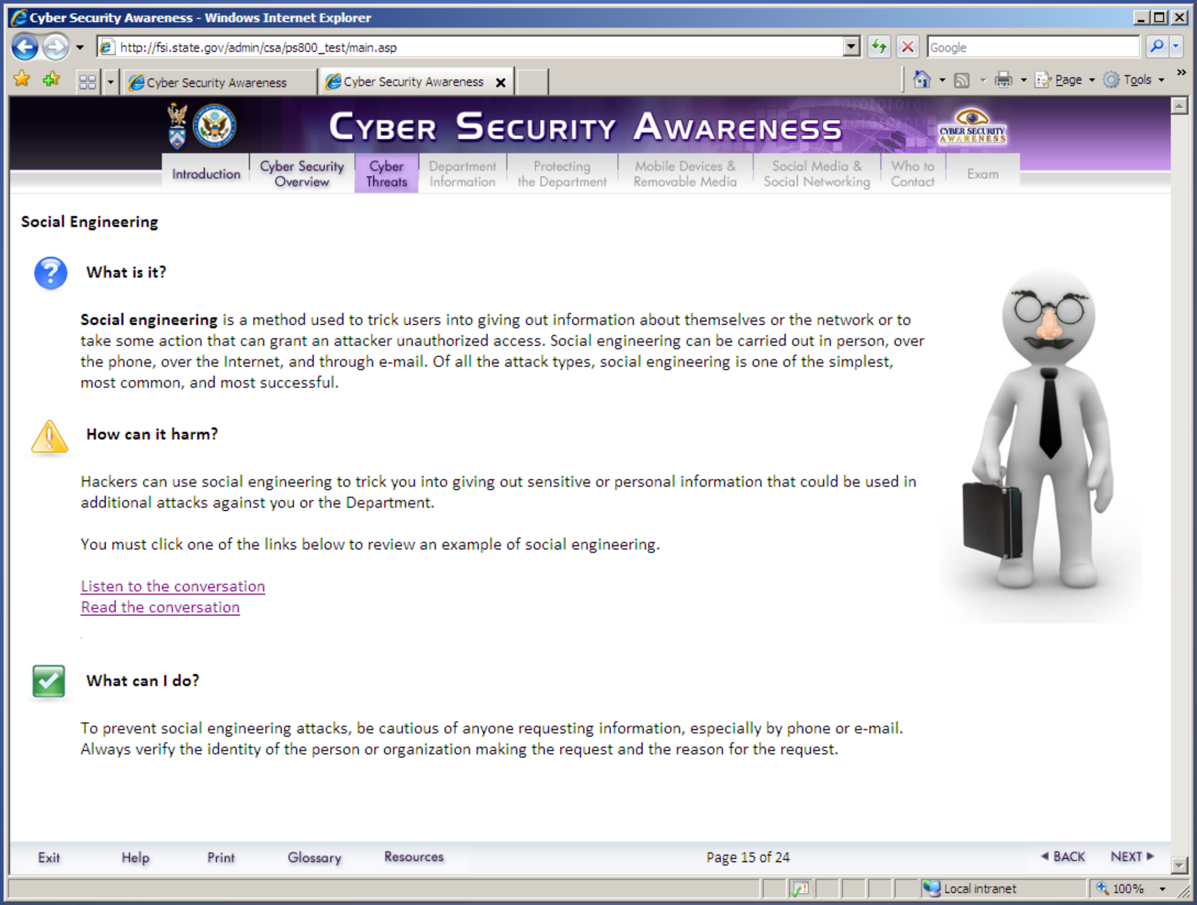
Version 4.0

Course Number: PS800

Select **Next** to continue.

Cybersecurity Awareness is a 45-minute web-based course requiring only an IE browser.

Interaction



Social Engineering

What is it?

Social engineering is a method used to trick users into giving out information about themselves or the network or to take some action that can grant an attacker unauthorized access. Social engineering can be carried out in person, over the phone, over the Internet, and through e-mail. Of all the attack types, social engineering is one of the simplest, most common, and most successful.

How can it harm?

Hackers can use social engineering to trick you into giving out sensitive or personal information that could be used in additional attacks against you or the Department.

You must click one of the links below to review an example of social engineering.

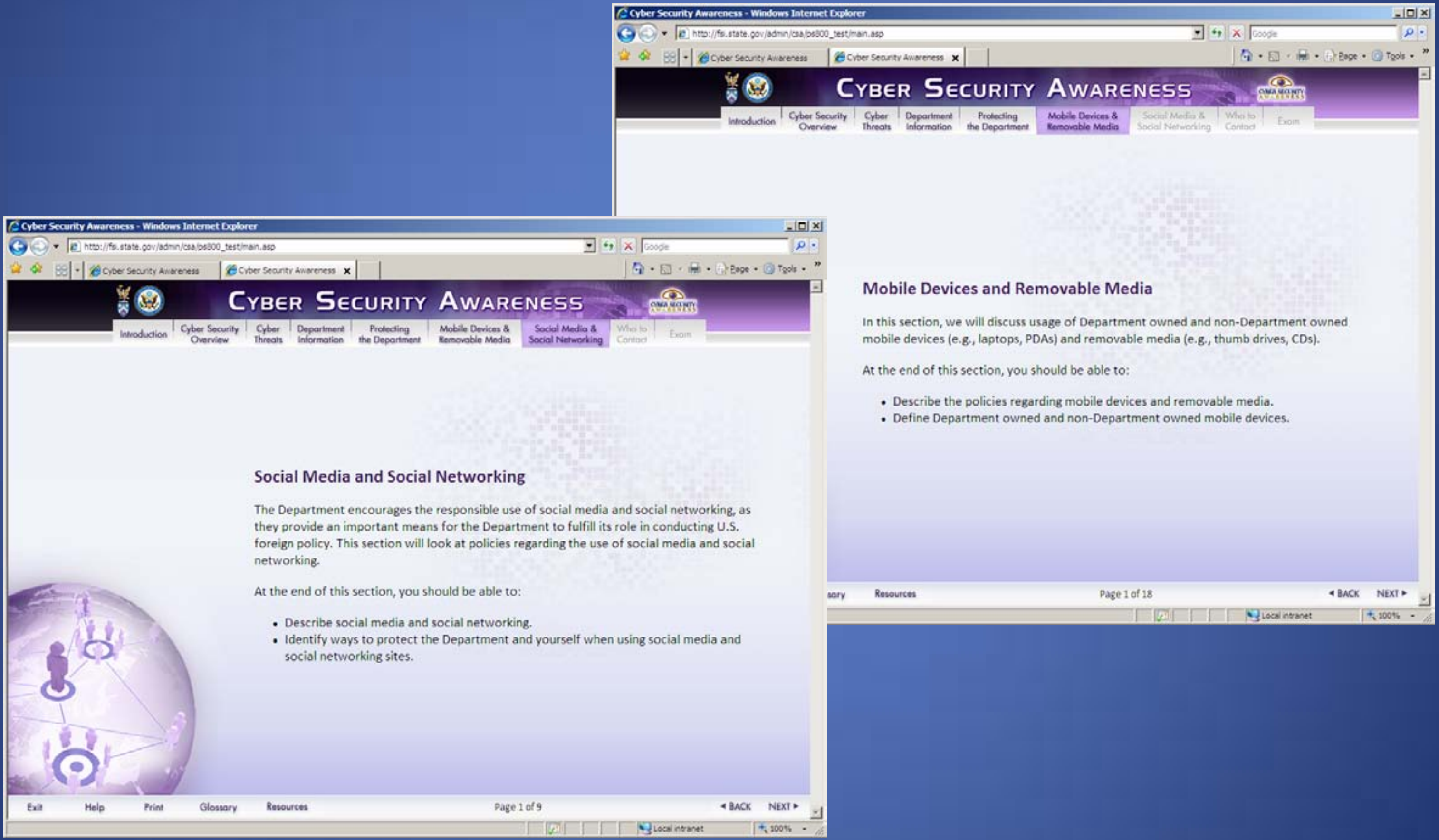
Listen to the conversation
Read the conversation

What can I do?

To prevent social engineering attacks, be cautious of anyone requesting information, especially by phone or e-mail. Always verify the identity of the person or organization making the request and the reason for the request.

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

Modern Considerations


Cyber Security Awareness - Windows Internet Explorer
http://fsi.state.gov/admin/csa/ps800_test/main.asp
Cyber Security Awareness
CYBER SECURITY AWARENESS
Introduction
Cyber Security Overview
Cyber Threats
Department Information
Protecting the Department
Mobile Devices & Removable Media
Social Media & Social Networking
Who to Contact
Exam
Resources
Page 1 of 18
BACK
NEXT
Local intranet
100%

Mobile Devices and Removable Media

In this section, we will discuss usage of Department owned and non-Department owned mobile devices (e.g., laptops, PDAs) and removable media (e.g., thumb drives, CDs).

At the end of this section, you should be able to:

- Describe the policies regarding mobile devices and removable media.
- Define Department owned and non-Department owned mobile devices.

Cyber Security Awareness - Windows Internet Explorer
http://fsi.state.gov/admin/csa/ps800_test/main.asp
CYBER SECURITY AWARENESS
Introduction
Cyber Security Overview
Cyber Threats
Department Information
Protecting the Department
Mobile Devices & Removable Media
Social Media & Social Networking
Who to Contact
Exam
Exit
Help
Print
Glossary
Resources
Page 1 of 9
BACK
NEXT
Local intranet
100%

Social Media and Social Networking

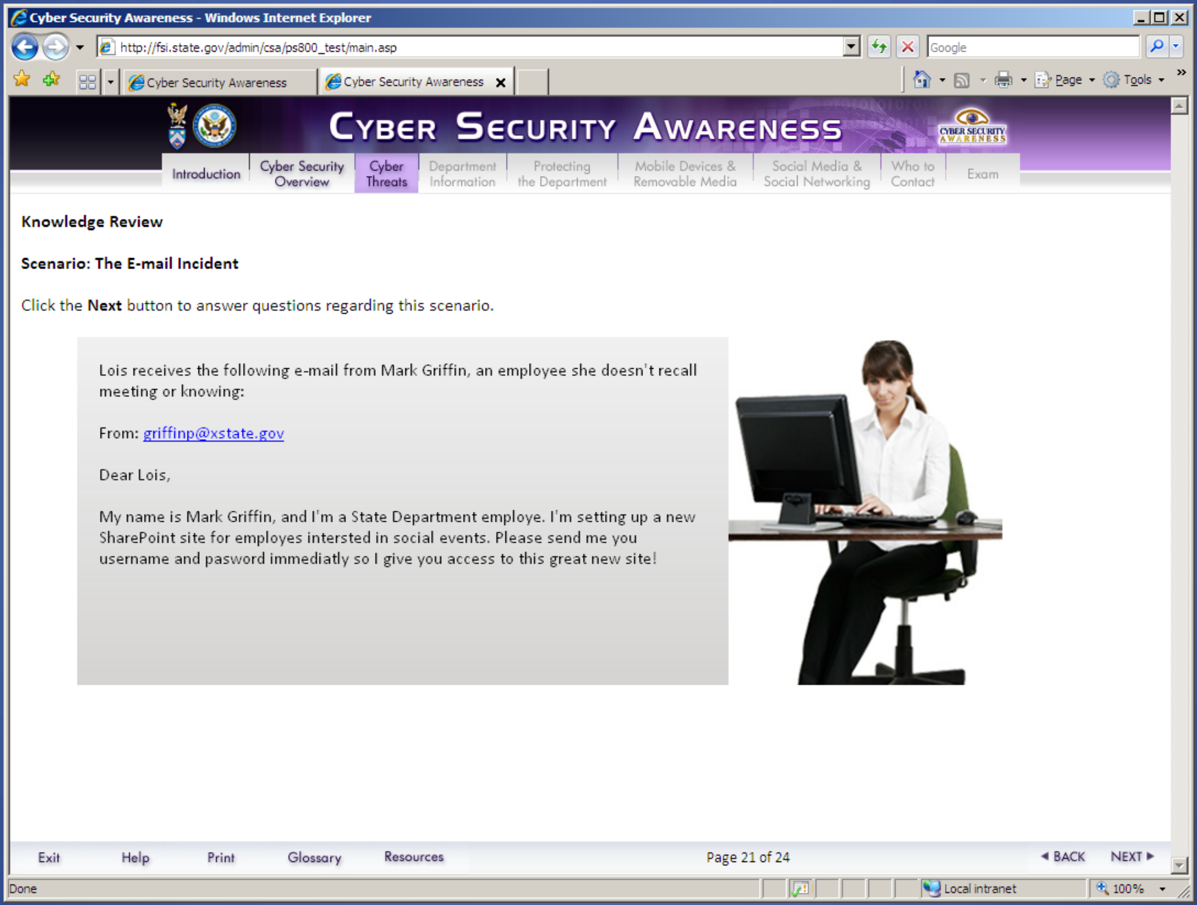
The Department encourages the responsible use of social media and social networking, as they provide an important means for the Department to fulfill its role in conducting U.S. foreign policy. This section will look at policies regarding the use of social media and social networking.

At the end of this section, you should be able to:

- Describe social media and social networking.
- Identify ways to protect the Department and yourself when using social media and social networking sites.

New technologies and media, such as mobile devices and social networking are addressed.

User Action and Response



Knowledge Review

Scenario: The E-mail Incident

Click the **Next** button to answer questions regarding this scenario.

Lois receives the following e-mail from Mark Griffin, an employee she doesn't recall meeting or knowing:

From: griffinp@xstate.gov

Dear Lois,

My name is Mark Griffin, and I'm a State Department employe. I'm setting up a new SharePoint site for employes intersted in social events. Please send me you username and pasword immediatly so I give you access to this great new site!

The end of each section includes review questions that ask learners to apply their knowledge to a scenario.

Cyber Security FY2011 Preview

- Increased user base and LMS implementations
- Revised content to give fresh look & feel
- Section on Mobile devices (Blackberry, iPad, Smartphones, etc.) and increase attention to social networking
- Review questions at the end of each section are set within the context of a scenario that asks the user what action to take, rather than simply asking them to remember information
- Revised/Updated test and review questions

Security Awareness Training

Security Tips of the Day

Deliver awareness.

Protect information.

DEPARTMENT OF STATE
UNITED STATES OF AMERICA

Department of State

Security Incidents Highlighted Need for Awareness

- USAID saw the need to develop new, more effective, security interactions

- Tips of the Day was created to provide a daily security interaction for improving security habits and reinforce security training

State Department-wide Deployment

- Currently in use by IRM and DS bureaus

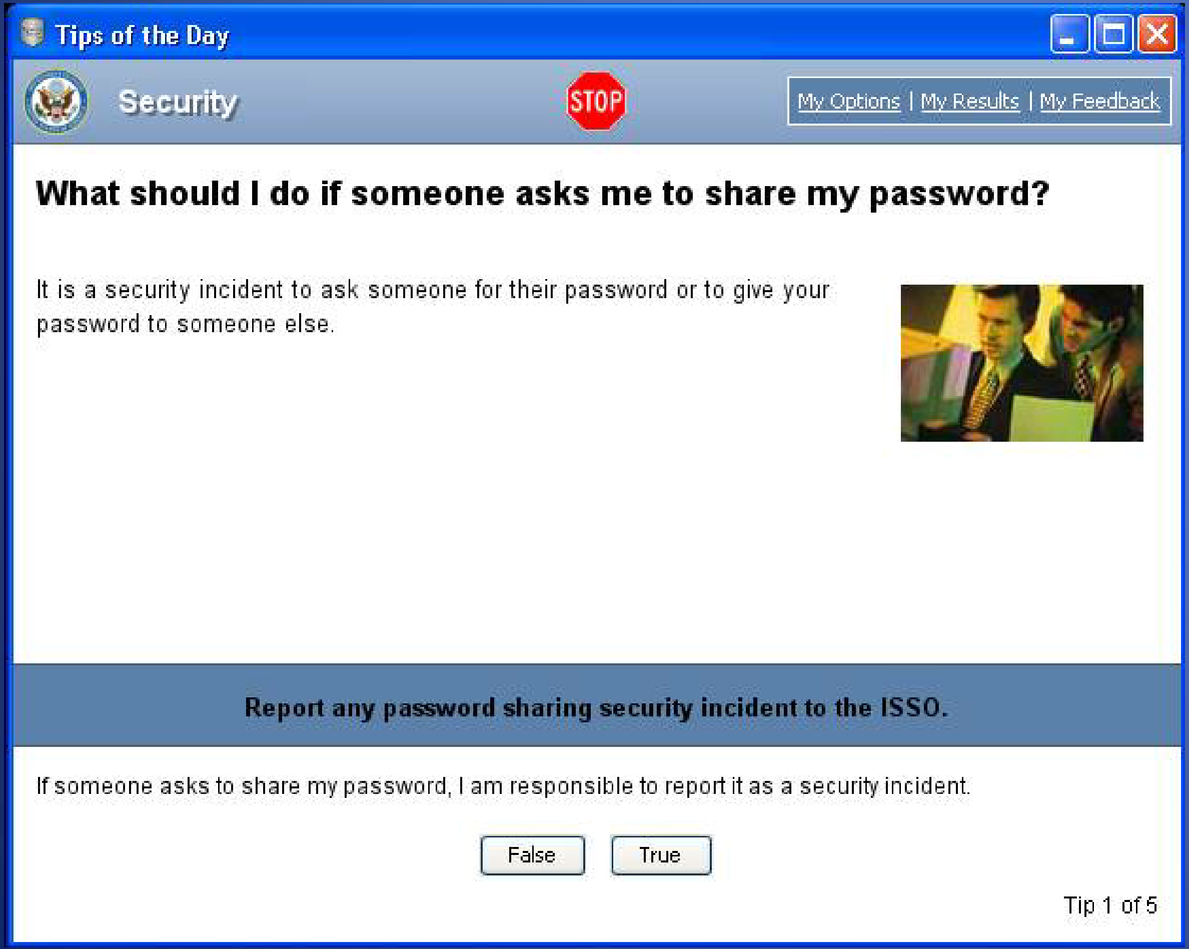
- Progressive deployment to rest of Department by June 2011

- Ultimately will be total of 70,000 TOD users

Others Using Tips of the Day

- Several departments and agencies have piloted or are evaluating TOD:
  - Department of Transportation
  - Department of Health and Human Services
  - Department of Defense
  - Department of Interior
  - US Courts
  - US Postal Service

TOD Operation and Features



What should I do if someone asks me to share my password?

It is a security incident to ask someone for their password or to give your password to someone else.

Report any password sharing security incident to the ISSO.

If someone asks to share my password, I am responsible to report it as a security incident.

Tip 1 of 5

- User logs into system and receives a tip.
- User reads the question and clicks one button to answer.
- No user navigation is required.
- Concise & actionable.
- Highly scalable.
- 508 compliant.
- Capable of providing role-targeted tips.

Teaming with Contactor

- TOD developer, Pragmatics Inc, provides the following services:
  - Installation support
  - Hosting
  - Content development
  - Tier 1, 2, and/or 3 Support
  - Piloting
  - Routine O&M

Contact for TOD

- Vickie L. McCray
- Program Manager – Pragmatics Inc.
- 703-812-2386
- mccrayv@pragmatics.com

JSAS Website

HTTP://JSAS.STATE.GOV