



Information Privacy and Security (IPAS)  
Web Conference | June 9, 2008

Mike Leach, Project Manager  
Jenn Stewart, Technical Coordinator



# Objectives

- Evolving Web Threats
- Early Stages of Phase II
- Take Charge
- Available Resources
- Summary
- Question & Answer Session



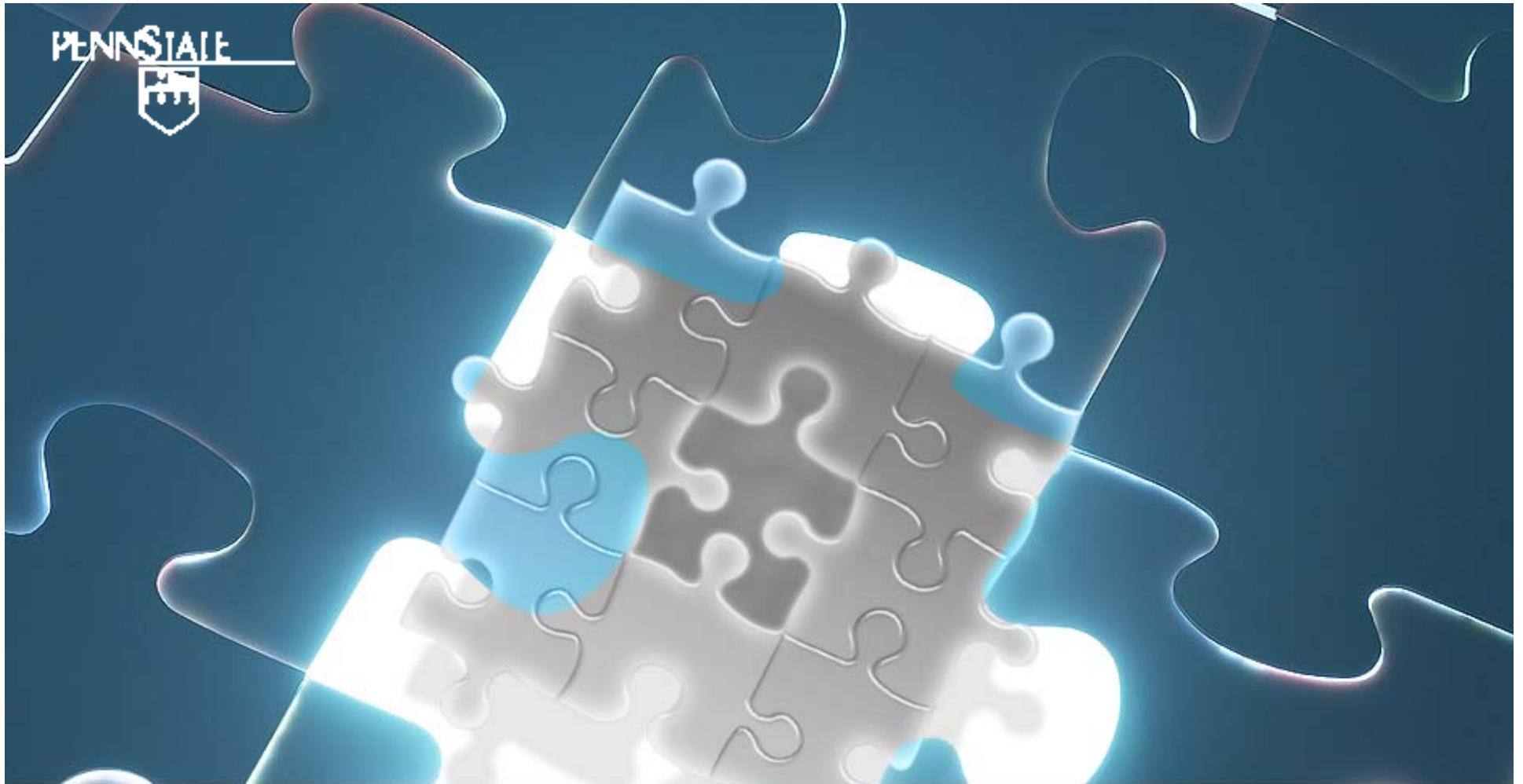
# Information Privacy and Security

- University-wide Mission
- Formed Fall 2006
- Support and Leadership
- Phase I Goals
- Phase II Goals



# Paradigm Shift

- Online Business
- Federal and State Statutes
- Research Agreements
- Contract and Business Agreements
- Penn State Policies



# **Evolving Threats**

**Statistics | Breach Examples | Reporting**



# Online Threats

- Botnets
- Man in the Middle
- Cross-site Scripting
- Worms
- Spyware
- Viruses
- Phishing scams
- Neglect



# Reporting

## Security Operations and Services (SOS)

- Suspicious activity
- Questions about email legitimacy
- Contact
  - Normal work hrs : 814-863-9533
  - After hrs: 814-777-9533

## Privacy Office (non-electronic concerns)

- 814 863 3049



# Statistics

- Total Loss of Records to date (2008):  
5,557,421
- Over 100 Breaches (2008)
- Approximate Remediation and  
Notification Cost/record \$197.00

*Record Loss Source: Privacy Rights Clearing  
House <http://www.privacyrights.org>*



# Data Breach Examples

A computer file containing the names and Social Security numbers of current and former Texas A&M University agricultural employees was **inadvertently posted online** and accessible to the public for three weeks.

Total Loss: 3,000

Feb. 16, 2008

Texas A&M University



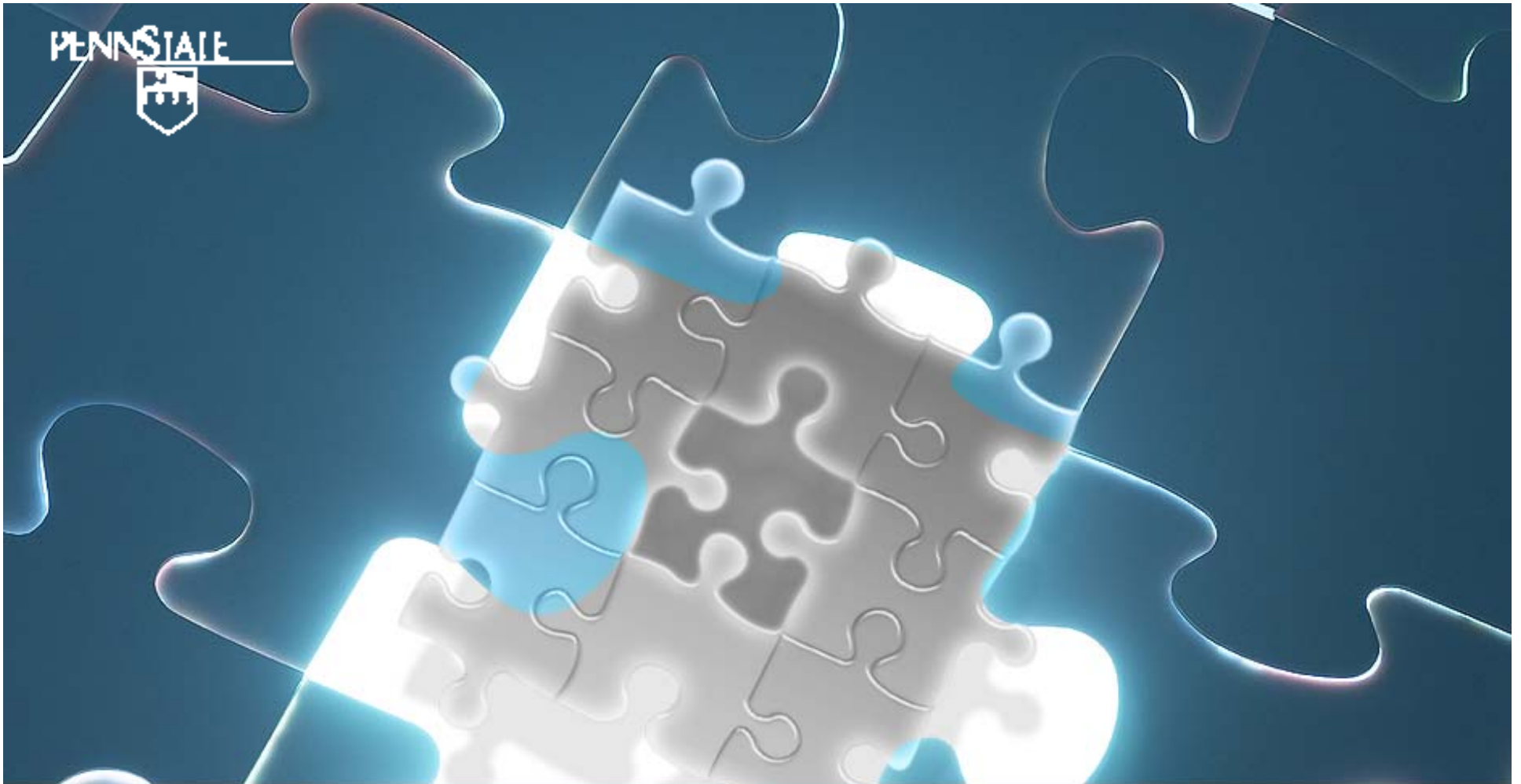
# Data Breach Examples

A university laptop containing archived information and Social Security numbers for 677 students attending Penn State between 1999 and 2004 was recently **stolen from a faculty member.**

Total Loss: 677

Jan. 25, 2008

**Penn State University**



## **Early Stages of Phase II**

**Data Classification | File Scanning | Encryption**



# Data Classification

- 2 Primary Classifications of Systems/Networks
  - Public
  - Non-Public
- 3 Primary Classifications of Data
  - Public
  - Internal/Controlled
  - Restricted



# Personally Identifiable Information

- Social Security Numbers
- Financial Information
- Credit Card Numbers
- Student Data
- Donor Information
- Legal Correspondence
- Personal Health Information

*...list not exhaustive*



# Data Classification Scheme

## Security Requirement Categories

Category 1: **Protection from the public Internet or external network segments** (direct probes)

Category 2: Systems connecting to the Penn State network will be **free from known vulnerabilities**



## Security Requirement Categories, continued

Category 3: Access to systems will be individually controlled. All actions must be traceable to a **unique user ID**.

Category 4: Access to systems and applications (beyond public display) **will be logged**.



## Security Requirement Categories, continued

Category 5: Data will be **secured at rest or in transit** commensurate with its sensitivity

Category 6: Sensitive data must be **sanitized or destroyed** prior to system re-use by another entity



## Security Requirement Categories, continued

Category 7: **Physical and facility security** must be maintained.

Category 8: A **development and risk assessment** process must be in place commensurate with the sensitivity of the data



## Security Requirement Categories, continued

Category 9: Units will **maintain local policies** in accordance with, and augmenting, University Policy AD20 (Computer and Network Security)

Category 10: **Backup and Disaster Recovery** measures must be in place commensurate with the value of the computer and network resources, and the data held

**2.3 Applications made accessible over the Web will be scanned for known web application vulnerabilities**

<b>Element</b>	<b>Technical Requirement</b>	<b>Public</b>	<b>Non-Public (Internal/Controlled or Restricted Information)</b>
2.3.1	Application Scan will be conducted by ITS for custom Web Applications	X	X
2.3.2	Application Level Firewall will be implemented		# (Mandatory for web applications hosting Restricted data)

# = measure is mandatory but implementation may not be possible due to immaturity of technology or other factors.



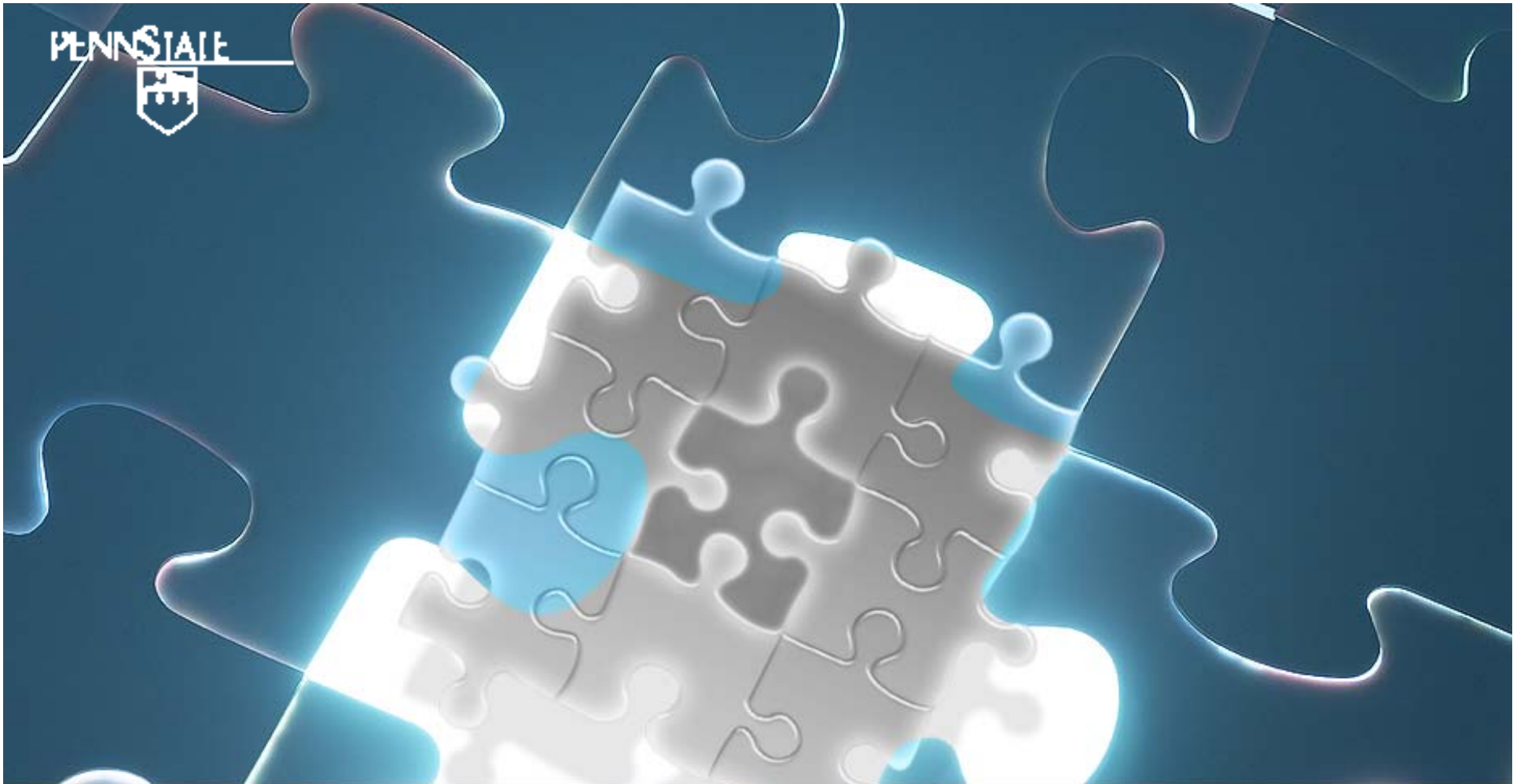
# File Scanning

- Goal: Detect sensitive information
- Beta Test with Select Units
- Implementation Fall 2008
- Details to Follow
  - Awareness Campaign



# Encryption

- Software: Utimaco's SafeGuard Easy
- Options: disk drive, mobile device
- Purpose: protect sensitive information
- Target:
  - all mobile devices
  - desktops in open environments
  - desktops processing PII
- Implementation: Fall 2008



# Take Charge

**Security Measures | Best Practices | Reporting**



# Secure Your Environment

- Hardware Firewall
- IDS/IPS
- Log Activity
- Encrypt Sensitive Information
- Keep all systems up to date
  - OS, antivirus, software/applications



# Best Practices

- Educate Yourself and Users
- Identify and Inventory
- Restrict Access
- Limit Administrative Privileges
- Separate Applications
- Request Scans Regularly
- Develop Local Policies



# Facing Challenges

- Adapting to Change
- Enforcement
- Funding
  - Device/system purchase
  - Implementation
  - Knowledge
  - Resources (staff)
  - On-going



# Available Resources

- IPAS Consulting
- SOS Scanning Services
- PSU eCommerce
- Tivoli Storage Manager
- ITS Firewall Services
- List Serves
- ITS Consultants
- My IT Community



# Summary

- Protect the Institution. WE are Penn State!
- Protect data Being Handled
- Meet On-going Compliance Obligations
- Limit Reportable Data Breaches
- Stay Tuned for Early Stages
- Enhance Business Practices at Penn State



# Links of Interest

- [www.ipas.psu.edu](http://www.ipas.psu.edu)
- [www.psu.edu/privacy](http://www.psu.edu/privacy)
- <http://sos.its.psu.edu/>
- <http://aset.its.psu.edu/accounts/tsm.html>
- <https://myit.vmhost.psu.edu/>
- [www.wikipedia.org/](http://www.wikipedia.org/)
- [www.privacyrights.org](http://www.privacyrights.org)
- [www.nist.gov/](http://www.nist.gov/)
- [www.sans.org/](http://www.sans.org/)



# Question and Answer Session

## Information Privacy and Security (IPAS)

814.867.1340

[www.ipas.psu.edu](http://www.ipas.psu.edu)

[ipas@psu.edu](mailto:ipas@psu.edu)