

# Information Privacy and Security (IPAS) Project

---

ITS Roadshow, Fayette  
April 30, 2008

Mike Leach, Project Manager

Craig Henninger, Senior Network Analyst

Jenn Stewart, Project Technical Coordinator

# Overview

---

## Phase II Early Stages

- Data Classification Scheme
- Sensitive Information Examples
- Scanning
- Encryption

# Data Classification (DC) Scheme

---

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

# Sensitive Information Examples

---

*(List not exhaustive)*

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

# Data Classification Scheme

## Security Requirement Categories

---

*(draft example of Security Requirements)*

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

# Data Classification Scheme

## Security Requirement Categories

---

*(draft example of Security Requirements)*

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

## Category 7: Physical and facility security must be maintained (draft example)

Element	Technical Requirement	Public	Non-Public (Internal/Controlled or Restricted Information)
7.1.1	Physically secured, locked space		
7.1.2	Employee identity proofing		
7.1.2	Logging of Visitors is required		
7.1.3	Escort of Visitors is required		
7.1.4	Surveillance cameras will be used and results routinely reviewed		

# Scanning Initiative

---

- Software: Proventsure's Governance and Compliance Platform
- Purpose: locate sensitive information
- Target: every computer
- Implementation: Fall 2008

# Scanning Process

---

1. Client installation – local IT staff
2. Scan is performed – local IT staff
3. Detected string results - IPAS server
  - Verification of results
4. Report issued to local IT staff
5. Sanitization of data - immediate

# Protected Information Report

Company: PSU

Department: [REDACTED]

**Computer:** [REDACTED]D152

<b>IP Address:</b>	172.28 [REDACTED]	<b>Credit Card:</b>	4
<b>O/S:</b>	Microsoft Windows NT 5.1.2600 Service Pack 2	<b>SSN:</b>	274
<b>Scan Policy:</b>	IPAS		
<b>Scan Date:</b>	2008-04-02 04:53:58		
<b>Assurance:</b>	24: Low Assurance		

## Confidential Data

**File Name:** C:\Asarium\logs\DefinedDataSearch.results

SSN	/DOS >> >> /59 6095 383 15 2482 8 9 0 [/ << / A [/ (
SSN	/EWHF S >> >> /11 1 204 35 8250 2 5 6 46 15 [/ << /
SSN	7580020 9 5 00020 9 544 57 0020 569 2 8 2 4002 00200
SSN	(266 76 L266 -66 -66 266 76 2664 76 266 -66 2664 76 2
SSN	03 03 903 03 103 303 403 03 2002 0020002003 403 10020
SSN	4 16 206 -06 2064 16 206 16 2064.06 -06 -06 306 16 30
SSN	6 160706 16 T706 -06 706 16 7060 16 706 7060 16 706W3
SSN	76 166 76 166 266 76 266 76 4266 -66 -66 L266 76\2664
SSN	8206 16 \206 -06 -06 206 16 2064 16 206 -06 2064 16 2
SSN	WHF S >> >> /6450 05 414 37 5401 1731286 9 [/ << / A
Totals:	SSN: 10

**File Name:** C:\dell\drivers\R111514\win2000\igfxnt5.cat

SSN	8086&DEV 2582&SUBSYS 019010280 + 7 0 HWID25 LPC\IVE
SSN	8086&DEV 2582&SUBSYS 019210280 + 7 0 HWID27 LPC\IVE
SSN	8086&DEV 2592&SUBSYS 018210280 + 7 0 HWID47 LPC\IVE
SSN	8086&DEV 2592&SUBSYS 018810280 + 7 0 HWID49 LPC\IVE
SSN	8086&DEV 2592&SUBSYS 019810280 + 7 0 HWID53 LPC\IVE
SSN	8086&DEV 2782&SUBSYS 019010280 + 7 0 HWID26 LPC\IVE
SSN	8086&DEV 2782&SUBSYS 019210280 + 7 0 HWID28 LPC\IVE
SSN	8086&DEV 2792&SUBSYS 018210280 + 7 0 HWID48 LPC\IVE
SSN	8086&DEV 2792&SUBSYS 018810280 + 7 0 HWID50 LPC\IVE
SSN	8086&DEV 2792&SUBSYS 019010280 + 7 0 HWID51 LPC\IVE
SSN	8086&DEV 2792&SUBSYS 019210280 + 7 0 HWID52 LPC\IVE

# 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 sensitive information
  - other
- Implementation: Fall 2008

# Benefits of Phase II

---

- Protect the institution
- Protect data being handled
  - Customers, students, donors, etc.
- Meet on-going compliance obligations
- Limit reportable data breaches
- Enhance business practices at Penn State

# Question and Answer Session

---

814.867.1340

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

<http://ipas.psu.edu>