

Information Classification Training

**NYS Office of Cyber Security and Critical
Infrastructure Coordination (CSCIC)**

**Sanjay Goel
Associate Professor, School of Business
University at Albany, SUNY**

Information Classification

Acknowledgements

- This presentation has been prepared by Prof. Sanjay Goel at the University at Albany, SUNY (UAlbany) in conjunction with the NYS Office of Cyber Security and Critical Infrastructure Coordination (CSCIC)
- The presentation uses material from the CSCIC Information Classification documents which were developed by Prof. Sanjay Goel and his team at UAlbany under contract with NYS CSCIC. Major contributors include:
 - Damira Pon, UAlbany
 - NYS CSCIC
 - NYS Information Classification Workgroup

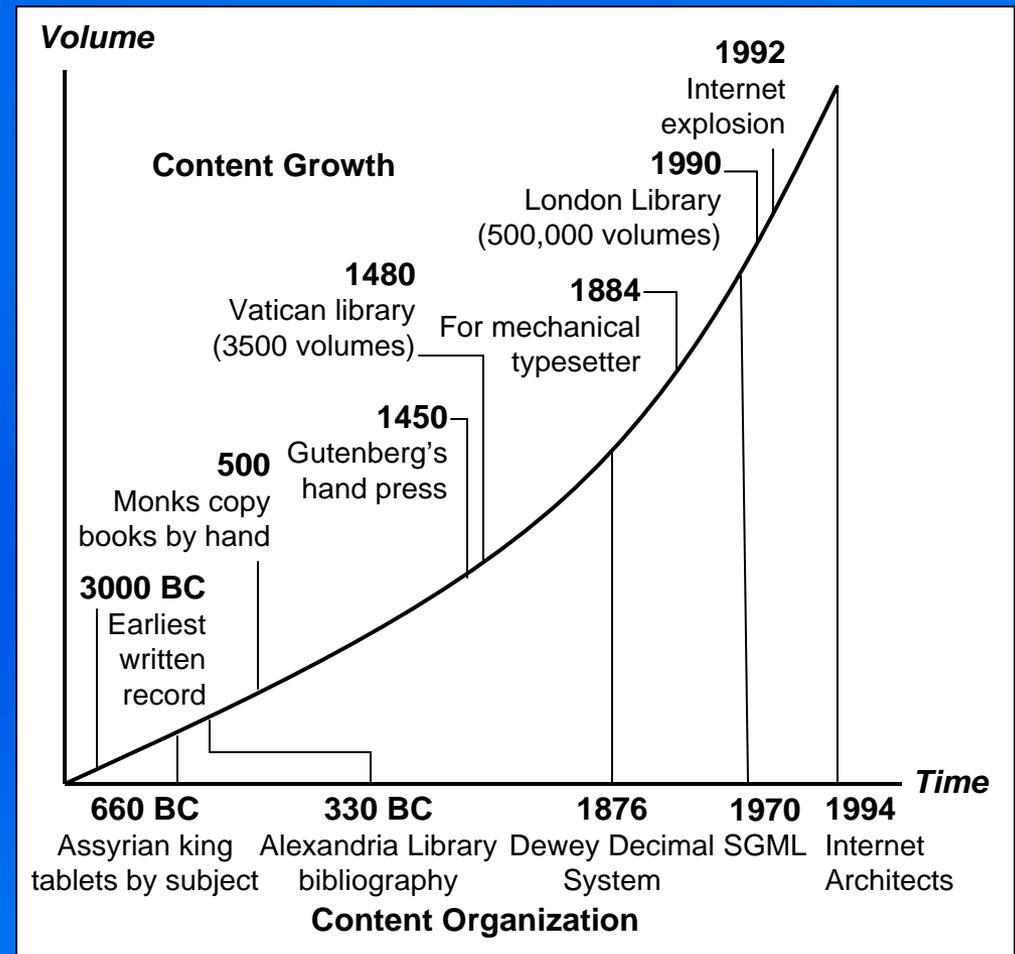
Goals & Objectives

- After the end of this training, you should:
 - Understand why information classification is important for overall security
 - Gain knowledge of how information is classified
 - Learn how to use CSCIC materials for information classification
 - Be able to perform information classification in your agency and identify baseline controls

Part I. Introduction to Information Classification

Information

- Information is a key organizational asset
- Information growth is constantly accelerating
- Same information can be stored in multiple places
- Organizations do not even know all the information that they possess

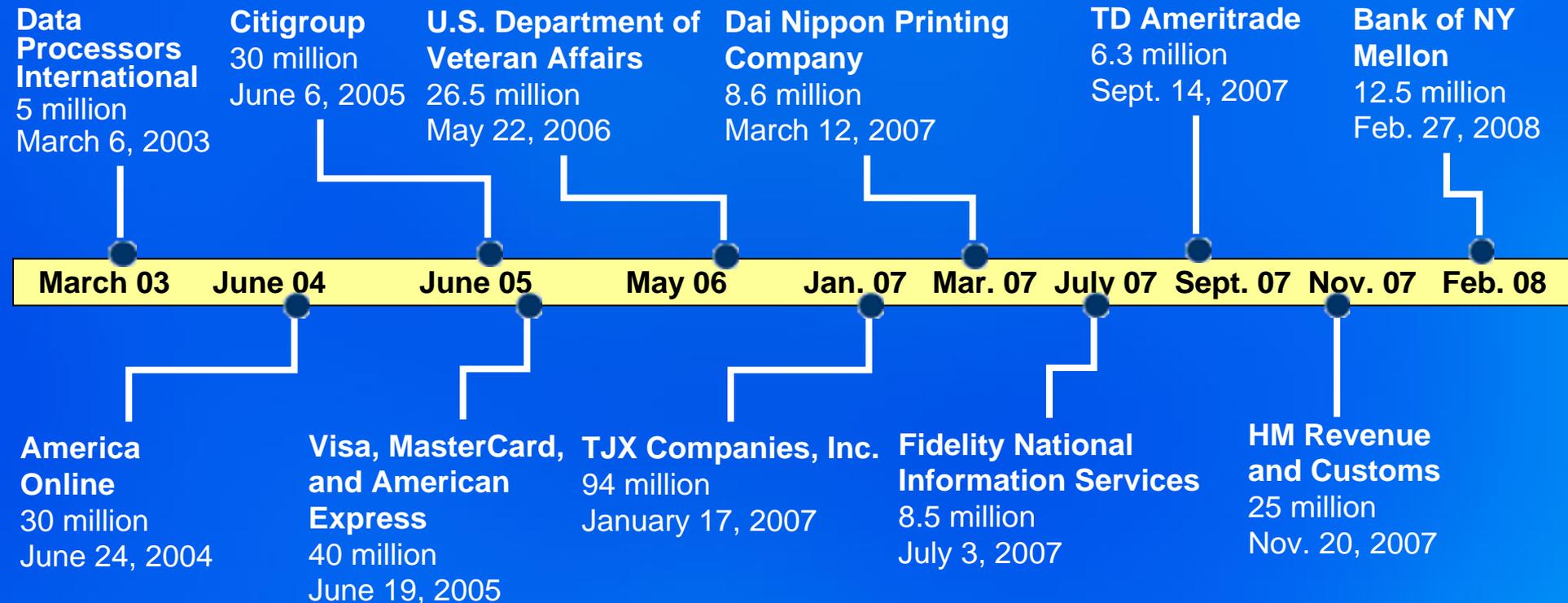


Source: O'Reilly

Why Protect Information?

- Information has inherent value and organizations need to protect this value
- Loss of information leads to
 - Loss of reputation and public trust
 - Loss of business/competitive edge
 - Loss of productivity
- Regulatory and industry pressure to secure information (SOX, HIPAA, FISMA, PCI, NYS ISBNA, etc.)
 - Non-compliance can result in fines and litigation
 - Notification costs (e.g., staff resources, financial)

Largest Data Breaches



Based on: Attrition Data Loss Archive and Database, FlowingData

Recent Government Data Breaches - 2009

- **Kanawha-Charleston Health Department, Charleston, WV (11,000 records – January 20th)**, personal information stolen by temporary worker
- **Indiana Department of Administration, Indianapolis, IN (8,775 records – January 30th)**, social security #'s posted on state website
- **University of Alabama, Tuscaloosa, AL (37,000 records – February 13th)**, seventeen databases tapped by hackers
- **Broome Community College, Binghamton, NY (14,000 records – February 17th)**, alumni magazine sent out with social security #'s printed on mailing labels
- **University of Florida, Gainesville, FL (97,200 records – February 19th)**, foreign hacker gained access to a computer system containing the personal information of students, faculty and staff
(previous breach in November, 2008 exposed 330,000 records)
- **Arkansas Department of Information Systems/Information Vaulting Services (807,000 records – February 20th)**, lost backup tape containing criminal background checks

Data Breaches Affecting NYS Residents

- Over 4 million NYS resident records have been breached since January 2007
- Estimated cost per record breached is \$202 including credit monitoring, forensics, legal defense, etc. (Source: 2008 Ponemon Study)
- We can estimate that NYS resident breaches would cost over \$808 million

Why Classify Information?

- Not all information requires same protection
 - Classification helps in establishing the value of information
 - Also helps in determining the level of protection required and in selection of appropriate controls



Image Source:

http://static.zoomr.com/images/369460_5df290cce5.jpg

Analyze Risk

- Information classification involves an understanding of the damage associated with data security breaches
- Damage can be evaluated by identifying
 - Loss associated with the breach
 - Likelihood that the breach will occur
- Classification is subjective
 - Different people have different perceptions of risk

Introduction to Information Classification

Key Points

- Information is a key organizational asset
- Needs to be protected for inherent value and regulatory compliance
- Need to understand the potential loss associated with data breaches
- This training class will help you understand how to analyze this risk and classify information

Part II. Information Classification Materials

How to Classify Data: Process

- Asset Identification
 - Inventory the data that the organization possesses
 - Group data that possesses similar characteristics
 - Identify the information owner and custodian
- Information Classification
 - Identify the impact of loss or unauthorized access to information on the following factors: Health and Safety, Mission/Programs, Public Trust & Reputation
 - For each group of data determine the level of protection required

How to Classify Data: Process Cont'd.

- Control Selection
 - Determine controls based on classification level
 - Perform a gap analysis with existing controls to determine additional controls required

NYS Information Classification

- CSCIC's Information Classification materials will make classification easier
 - Provide templates to inventory information assets, identify owners, and defines roles
 - Provide guidelines to help classify the data
 - Provide controls to ensure adequate protection of information

Let's see what materials we have...

Components

- **Information Classification Policy & Standard**
provides purpose, goals, roles, classification levels, and definitions & acronyms
- **Exemption Request Form (Appendix A)**
- **Information Classification Manual (Appendix B)**
describes the classification process with guidelines and examples
- **Information Asset Identification Worksheet (Appendix C, Page 1)** provides a template for collecting information during data inventory

Components, cont'd.

- **Information Asset Classification Worksheet (Appendix C, Page 2)** provides a series of questions to assist information owners in determining the classification levels
- **Information Control Charts (Appendix D)** specify baseline controls based on the classification
- **Glossary of Information Security Controls (Appendix E)** contains definitions for each control

Policy: Scope

- Policy applies to all information regardless of how it is stored and used
- Scope includes information through its entire life cycle (i.e., generation, use, storage and destruction)
- Covers information in all forms including electronic, paper, voice, and video

Policy: Scope

- Policy complements other NYS laws affecting information, e.g., Arts & Cultural Affairs Law (State Archives Records Retention), FOIL
- Protecting *information* is a shared responsibility
 - Each person may have more than one role and several people may act in the same role
 - In cases where the responsibility is divided among multiple individuals or groups, there should be a clear delineation of responsibilities

Stakeholders: Who are They?

- State Entities (SE): include all state agencies, departments, offices, divisions, boards, bureaus, commissions, and other entities over which the Governor has executive power. It also includes, SUNY Central Administration, CUNY Central Administration, and public benefit corps with heads appointed by the Governor
- SE Workforce: State employees and other persons whose conduct, in performance of work for the SE, is under direct control of the SE

Stakeholders

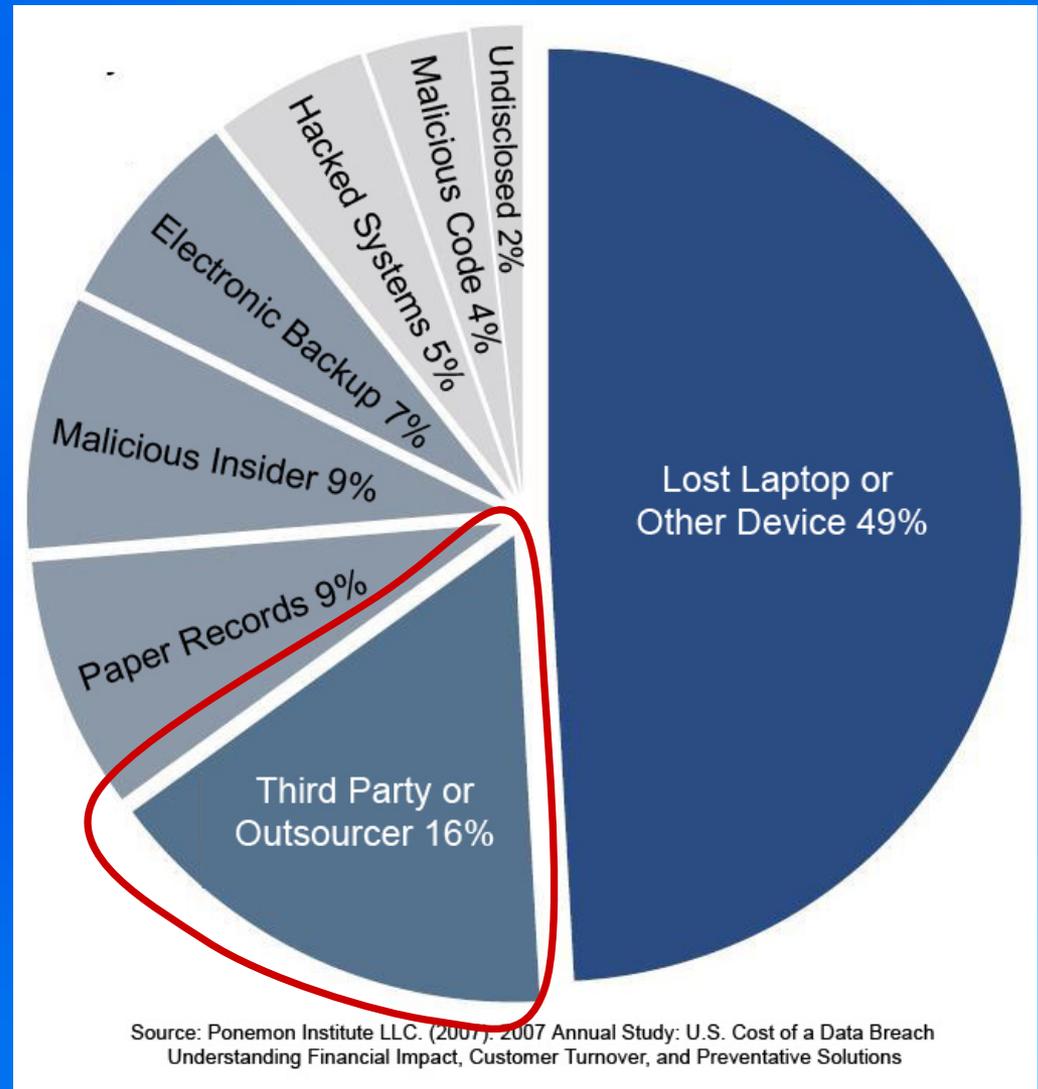
- Information Owner: Individual that has responsibility for making classification and access control decisions for information
- Information Custodian: Individual, organizational unit, or entity acting as caretaker of information on behalf of its owner
- Information Security Officer (ISO): A designated officer responsible for information security management in the SE

Stakeholders: SE/Management

- Information classification requires support of the entire organization
- Management support is critical to get buy-in from the organization
- Agency heads have been notified of the importance of this initiative

Stakeholders: Third Party

- Policy requirements must be addressed in third-party agreements as they relate to agency data
- If a third-party stores agency data, the agency is responsible for communicating requirements of the policy and standard to the third-party



Dimensions of Security

Confidentiality (C)
Information is not
disclosed without
authorization
(Privacy)



Integrity (I)
Information is not
accidentally or
maliciously altered
(Trust)

Availability (A)
Information is
available when
needed (Opportunity
Cost)

Levels of Classification

Consider impact of:

- unauthorized disclosure (C),
- modification/destruction (I) of data,
- loss of access (A)

on factors such as:

- Health and Safety
- Financial Loss
- Agency Mission/Programs
- Public Trust
- Legal Liability

Low

Minimal or no impact to the organization, its critical functions, workforce, business partners and/or its customers.

Mod.

Limited impact to the organization, its critical functions, workforce, business partners and/or its customers.

High

Severe impact to the organization, its critical functions, workforce, business partners and/or its customers.

Information Asset Classification Matrix

DIMENSIONS	LEVELS		
	LOW	MODERATE	HIGH
CONFIDENTIALITY	No to Minimal Impact	Limited Impact	Severe Impact
INTEGRITY	No to Minimal Impact	Limited Impact	Severe Impact
AVAILABILITY	No to Minimal Impact	Limited Impact	Severe Impact

Information Classification Materials

Key Points

- Classification involves information asset identification, classification, & control selection
- Classification decisions should be independent of the media (paper, tapes, computers, emails)
- Multiple stakeholders have specific roles in information classification process
- The policy defines 3 dimensions (C, I, A) and 3 levels (L, M, H) of classification

Part III. Information Classification Process

Information Asset Identification

- Information assets: All categories of information (both automated and non-automated) including data contained in records, files, and databases
- Information Asset Identification involves
 - 1) Asset Inventory
 - 2) Grouping Assets
 - 3) Information Owner /Custodian Identification

Information Asset Inventory

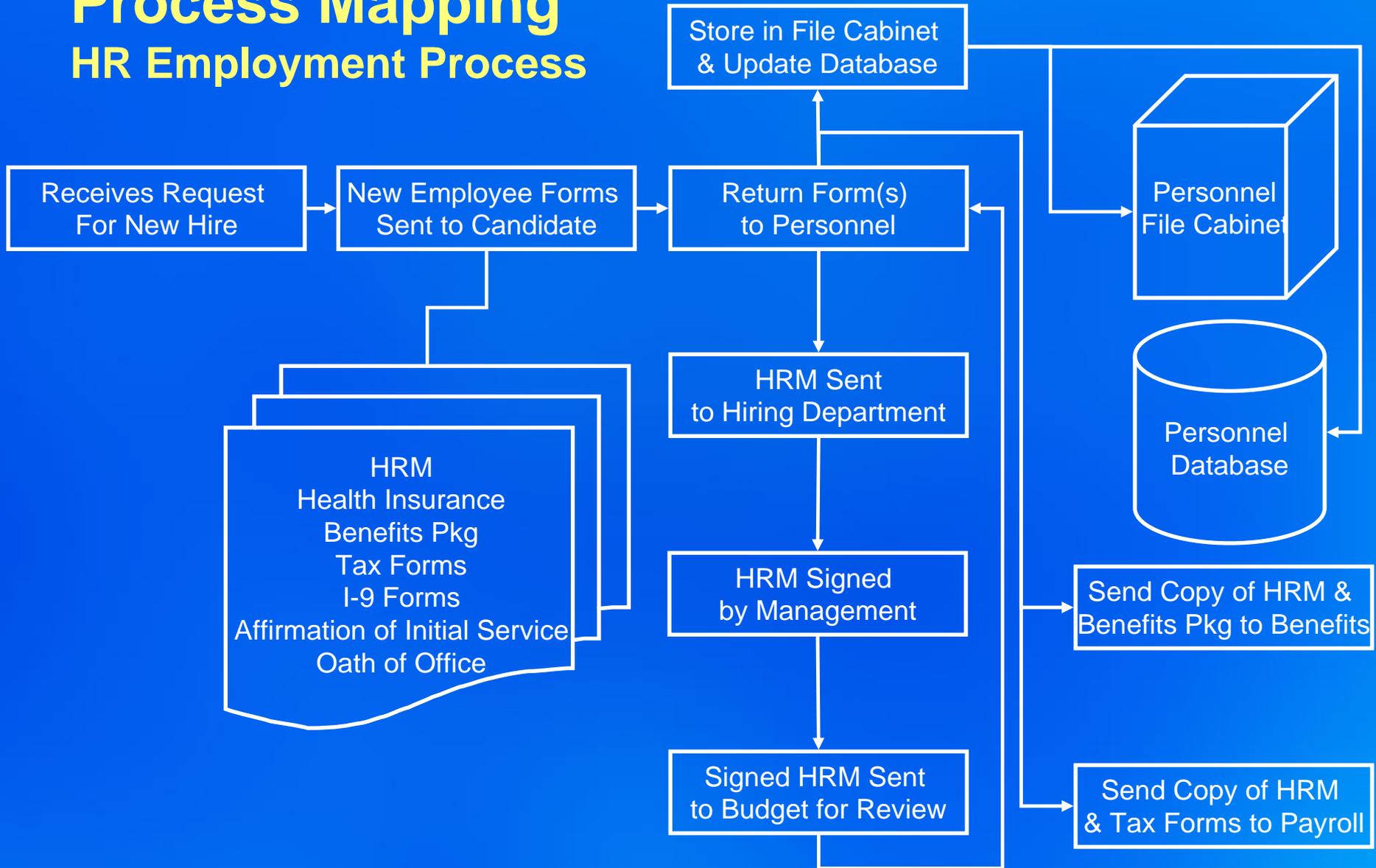
- Each business unit should be involved in identifying their own data
- Process should start with unit head/leader
- Information asset inventories currently in place can be used as a basis
 - Many agencies have inventories created for records management / preservation purposes

Grouping of Information Assets

- Effort involved in classification of information assets can be reduced by grouping of assets
- Data with similar security requirements may be grouped together as a single asset
 - e.g. all purchase requisition forms in the organization may be grouped
 - e.g. Data is sometimes grouped by systems (e.g. server, database, data warehouses)
- Grouping may not always be efficient
 - e.g. Grouping all data in a file cabinet may result in high confidentiality for all data even if a single page has personal confidential information

Process Mapping

HR Employment Process



Information Asset Identification

- Agencies must keep a repository of information assets
- Clear distinction between custodian, owner, and user
- Source could be internal or external
- Agency should define a numbering scheme

Completed By:
Completed Date:
Department:
Department Head:
Name of Information Asset:
Information Asset Use:
Information Asset Format:
Information Asset Storage:
Source of Information:
Business Process(es) Supported:
Information Owner:
Information Custodian:
Internal Information User(s):
External Information User(s):
Unique Information Asset ID Number:

Identifying the Owner

- The information owner is a person who makes decisions on information access (who, when, and how)
 - Typically owner should be an individual in a managerial position
- If multiple individuals are found to be potential “owners” of the same information, a single individual should be designated as the information “owner” by management
- In case of shared ownership of data the responsibility should be clearly delineated
- Owner may consult with subject matter experts for assistance in classifying information

Identifying the Custodian

- Information custodians are people, units, or organizations responsible for implementing the authorized controls to information assets based on the classification level
- Information custodians can be from within the SE or a third party
- Information owner and custodian can be the same person (e.g. network security logs)
- Information owner and user can also be the same person (e.g. information stored on a personal computer instead of the network)

Asset Identification Sheet

HRM Form

Completed By: Peter Pan
Completed Date: October 23, 2008
Department: HR Department
Department Head: Tinker Bell
Name of Information Asset: HRM Form
Information Asset Use: Hiring, Payroll, Benefits
Information Asset Format: Paper / Electronic
Information Asset Storage: HR File Cabinet, HR Database
Source of Information: Employee
Business Processes Supported: Hiring, Budget, Payroll
Information Owner: Tinker Bell
Information Custodian: ITS / HR Department
Etc....

Personnel File Group
(HRM Form, I-9 Form,
IT-2104/W-4, Affirmation of
Initial Service, Oath of Office,
Benefits Forms)

- Information can be grouped, e.g. instead of just the HRM form, the entire Personnel File Group can be an information asset

Classifying the Information

- Information Owner is responsible for completing classification
- Classification done using Information Classification Worksheet
 - Provides easy to use template for classifying data
 - Contains questions for all security dimensions (C, I, A) which are evaluated on impact level
- Worksheet should be used with Information Classification Manual
 - Provides guided questions and examples

Information Classification Worksheet

Cyber Security Policy & Standard PS08-001
Unique Information Asset ID Number:

INFORMATION ASSET CLASSIFICATION WORKSHEET CIA QUESTIONS

Appendix C

CONFIDENTIALITY QUESTIONS	INTEGRITY QUESTIONS	AVAILABILITY QUESTIONS
<p>1 Does the information include or contain PPSI (Personal, Private, or Sensitive Information)?</p> <p>A) No - continue with Confidentiality questions D) Yes - Confidentiality is High (rate below), continue with Integrity questions</p>	<p>1 Does the information include medical records?</p> <p>A) No - continue with Integrity questions D) Yes - Integrity is High (rate below), continue with Availability questions</p>	<p>1 Is availability of the information essential for emergency response or disaster recovery?</p> <p>A) No - continue with Availability questions D) Yes - Availability is High (rate below)</p>
<p>2 What impact does unauthorized access or disclosure of information have on health and safety?</p> <p>A) None - continue with Confidentiality questions B) Minimal impact - continue with Confidentiality questions C) Limited impact - continue with Confidentiality questions D) Severe impact - Confidentiality is High (rate below), continue with Integrity questions</p>	<p>2 Is the information (e.g., security logs) relied upon to make critical security decisions?</p> <p>A) No - continue with Integrity questions D) Yes - Integrity is High (rate below), continue with Availability questions</p>	<p>2 This information needs to be provided or available:</p> <p>A) As time permits - continue with Availability questions C) Within 1 to 7 days - continue with Availability questions D) 24 hrs. per day/7 days a week - Availability is High (rate below)</p>
<p>3 What is the financial impact of unauthorized access or disclosure of information?</p> <p>A) None - continue with Confidentiality questions B) Minimal impact - continue with Confidentiality questions C) Limited impact - continue with Confidentiality questions D) Severe impact - Confidentiality is High (rate below), continue with Integrity questions</p>	<p>3 What impact does unauthorized modification or destruction of information have on health and safety?</p> <p>A) None - continue with Integrity questions B) Minimal impact - continue with Integrity questions C) Limited impact - continue with Integrity questions D) Severe impact - Integrity is High (rate below), continue with Availability questions</p>	<p>3 What is the impact to health and safety if information were not available when needed?</p> <p>A) None - continue with Availability questions B) Minimal impact - continue with Availability questions C) Limited impact - continue with Availability questions D) Severe impact - Availability is High (rate below)</p>
<p>4 What impact does unauthorized access or disclosure of information have on the SE mission?</p> <p>A) None - continue with Confidentiality questions B) Minimal impact - continue with Confidentiality questions C) Limited impact - continue with Confidentiality questions D) Severe impact - Confidentiality is High (rate below), continue with Integrity questions</p>	<p>4 What is the financial impact of unauthorized modification or destruction of information?</p> <p>A) None - continue with Integrity questions B) Minimal impact - continue with Integrity questions C) Limited impact - continue with Integrity questions D) Severe impact - Integrity is High (rate below), continue with Availability questions</p>	<p>4 What is the financial impact if information were not available when needed?</p> <p>A) None - continue with Availability questions B) Minimal impact - continue with Availability questions C) Limited impact - continue with Availability questions D) Severe impact - Availability is High (rate below)</p>
<p>5 What impact does unauthorized access or disclosure of information have on the public trust?</p> <p>A) None - continue with Confidentiality questions B) Minimal impact - continue with Confidentiality questions C) Limited impact - continue with Confidentiality questions D) Severe impact - Confidentiality is High (rate below), continue with Integrity questions</p>	<p>5 What impact does unauthorized modification or destruction of information have on the SE mission?</p> <p>A) None - continue with Integrity questions B) Minimal impact - continue with Integrity questions C) Limited impact - continue with Integrity questions D) Severe impact - Integrity is High (rate below), continue with Availability questions</p>	<p>5 What is the impact to the SE mission if information were not available when needed?</p> <p>A) None - continue with Availability questions B) Minimal impact - continue with Availability questions C) Limited impact - continue with Availability questions D) Severe impact - Availability is High (rate below)</p>
<p>6 Is confidentiality mandated by law or regulation? If yes, determine the impact of unauthorized access or disclosure of information.</p> <p>A) No - continue with Confidentiality questions B) Yes - Minimal impact - continue with Confidentiality questions C) Yes - Limited impact - continue with Confidentiality questions D) Yes - Severe impact - Confidentiality is High (rate below), continue with Integrity questions</p>	<p>6 What impact does unauthorized modification or destruction of information have on the public trust?</p> <p>A) None - continue with Integrity questions B) Minimal impact - continue with Integrity questions C) Limited impact - continue with Integrity questions D) Severe impact - Integrity is High (rate below), continue with Availability questions</p>	<p>6 What is the impact to the public trust if the information were not available when needed?</p> <p>A) None - see Instructions below B) Minimal impact - see Instructions below C) Limited impact - see Instructions below D) Severe impact - Availability is High (rate below)</p>
<p>7 Is the information intended for limited distribution? If yes, determine the impact of unauthorized access or disclosure.</p> <p>A) No - continue with Confidentiality questions B) Yes - Minimal impact - continue with Confidentiality questions C) Yes - Limited impact - continue with Confidentiality questions D) Yes - Severe impact - Confidentiality is High (rate below), continue with Integrity questions</p>	<p>7 Is integrity addressed by law or regulation? If yes, determine the impact of unauthorized modification or destruction of information.</p> <p>A) No - continue with Integrity questions B) Yes - Minimal impact - continue with Integrity questions C) Yes - Limited impact - continue with Integrity questions D) Yes - Severe impact - Integrity is High (rate below), continue with Availability ques.</p>	
<p>8 Is the information publicly available?</p> <p>A) No - see Instructions below, then continue with Integrity questions B) Yes - see Instructions below, then continue with Integrity questions</p>	<p>8 Is the information (e.g., financial transactions, performance appraisals) relied upon to make business decisions? If yes, determine the impact of unauthorized modification or destruction of information.</p> <p>A) No - see Instructions below then continue with Availability questions B) Yes - Minimal impact - see Instructions below then continue with Availability ques. C) Yes - Limited impact - see Instructions below then continue with Availability ques. D) Yes - Severe impact - Integrity is High (rate below), continue with Availability ques.</p>	
<p>INSTRUCTIONS FOR RATING EACH COLUMN: If ALL of the above answers are A) (GREEN), rating is LOW; if ANY of the above answers are C) (YELLOW) and NONE are D) (RED), rating is MODERATE; if ANY of the above answers are D) (RED), rating is HIGH SCALE: A/B = GREEN = LOW C = YELLOW = MODERATE D = RED = HIGH</p>		
<p>CLASSIFICATION RATING FOR CONFIDENTIALITY: V1.1 December 4, 2008</p>	<p>CLASSIFICATION RATING FOR INTEGRITY:</p>	<p>CLASSIFICATION RATING FOR AVAILABILITY:</p>

Information Classification Manual

Information Classification and Control Appendix B

Information Classification Manual

Original Publication Date: October 10, 2008
Revision Date: December 4, 2008

- **Confidentiality Questions**
- [1] Does the information include or contain PPSI (Personal, Private or Sensitive Information)?
- **Example(s):** A W-2 form contains a name, as well as a social security number. This would be considered private information and therefore have a confidentiality of high. See the Definitions & Acronyms section of the Information Classification and Control Policy and Standard (PS08-001) for a definition of PPSI.

Using the Worksheet – HRM Form Example

CONFIDENTIALITY QUESTIONS	INTEGRITY QUESTIONS	AVAILABILITY QUESTIONS
<p>1 Does the information include or contain PPSI (Personal, Private, or Sensitive Information)?</p> <p>A) No - continue with Confidentiality questions D) Yes - Confidentiality is High (rate below), continue with Integrity questions</p>	<p>1 Does the information include medical records?</p> <p>A) No - continue with Integrity questions D) Yes - Integrity is High (rate below), continue with Availability questions</p>	<p>1 Is availability of the information essential for emergency response or disaster recovery?</p> <p>A) No - continue with Availability questions D) Yes - Availability is High (rate below)</p>
<p>2 What impact does unauthorized access or disclosure of information have on health and safety?</p> <p>A) None - continue with Confidentiality questions B) Minimal impact - continue with Confidentiality questions C) Limited impact - continue with Confidentiality questions D) Severe Impact - Confidentiality is High (rate below), continue with Integrity questions</p>	<p>2 Is the information (e.g., security logs) relied upon to make critical security decisions?</p> <p>A) No - continue with Integrity questions D) Yes - Integrity is High (rate below), continue with Availability questions</p>	<p>2 This information needs to be provided or available:</p> <p>A) As time permits - continue with Availability questions C) Within 1 to 7 days - continue with Availability questions D) 24 hrs. per day/7 days a week - Availability is High (rate below)</p>
<p>3 What is the financial impact of unauthorized access or disclosure of information?</p> <p>A) None - continue with Confidentiality questions B) Minimal impact - continue with Confidentiality questions C) Limited impact - continue with Confidentiality questions D) Severe Impact - Confidentiality is High (rate below), continue with Integrity questions</p>	<p>3 What impact does unauthorized modification or destruction of information have on health and safety?</p> <p>A) None - continue with Integrity questions B) Minimal impact - continue with Integrity questions C) Limited impact - continue with Integrity questions D) Severe Impact - Integrity is High (rate below), continue with Availability questions</p>	<p>3 What is the impact to health and safety if information were not available when needed?</p> <p>A) None - continue with Availability questions B) Minimal impact - continue with Availability questions C) Limited impact - continue with Availability questions D) Severe Impact - Availability is High (rate below)</p>
<p>4 What impact does unauthorized access or disclosure of information have on the SE mission?</p> <p>A) None - continue with Confidentiality questions B) Minimal impact - continue with Confidentiality questions C) Limited impact - continue with Confidentiality questions D) Severe Impact - Confidentiality is High (rate below), continue with Integrity questions</p>	<p>4 What is the financial impact of unauthorized modification or destruction of information?</p> <p>A) None - continue with Integrity questions B) Minimal impact - continue with Integrity questions C) Limited impact - continue with Integrity questions D) Severe Impact - Integrity is High (rate below), continue with Availability questions</p>	<p>4 What is the financial impact if information were not available when needed?</p> <p>A) None - continue with Availability questions B) Minimal impact - continue with Availability questions C) Limited impact - continue with Availability questions D) Severe Impact - Availability is High (rate below)</p>
<p>5 What impact does unauthorized access or disclosure of information have on the public trust?</p> <p>A) None - continue with Confidentiality questions B) Minimal impact - continue with Confidentiality questions C) Limited impact - continue with Confidentiality questions D) Severe Impact - Confidentiality is High (rate below), continue with Integrity questions</p>	<p>5 What impact does unauthorized modification or destruction of information have on the SE mission?</p> <p>A) None - continue with Integrity questions B) Minimal impact - continue with Integrity questions C) Limited impact - continue with Integrity questions D) Severe Impact - Integrity is High (rate below), continue with Availability questions</p>	<p>5 What is the impact to the SE mission if information were not available when needed?</p> <p>A) None - continue with Availability questions B) Minimal impact - continue with Availability questions C) Limited impact - continue with Availability questions D) Severe Impact - Availability is High (rate below)</p>
<p>6 Is confidentiality mandated by law or regulation? If yes, determine the impact of unauthorized access or disclosure of information.</p> <p>A) No - continue with Confidentiality questions B) Yes - Minimal impact - continue with Confidentiality questions C) Yes - Limited impact - continue with Confidentiality questions D) Yes - Severe impact - Confidentiality is High (rate below), continue with Integrity questions</p>	<p>6 What impact does unauthorized modification or destruction of information have on the public trust?</p> <p>A) None - continue with Integrity questions B) Minimal impact - continue with Integrity questions C) Limited impact - continue with Integrity questions D) Severe impact - Integrity is High (rate below), continue with Availability questions</p>	<p>6 What is the impact to the public trust if the information were not available when needed?</p> <p>A) None - see Instructions below B) Minimal impact - see Instructions below C) Limited impact - see Instructions below D) Severe impact - Availability is High (rate below)</p>
<p>7 Is the information intended for limited distribution? If yes, determine the impact of unauthorized access or disclosure.</p> <p>A) No - continue with Confidentiality questions B) Yes - Minimal impact - continue with Confidentiality questions C) Yes - Limited impact - continue with Confidentiality questions D) Yes - Severe impact - Confidentiality is High (rate below), continue with Integrity questions</p>	<p>7 Is integrity addressed by law or regulation? If yes, determine the impact of unauthorized modification or destruction of information.</p> <p>A) No - continue with Integrity questions B) Yes - Minimal impact - continue with Integrity questions C) Yes - Limited impact - continue with Integrity questions D) Yes - Severe impact - Integrity is High (rate below), continue with Availability questions.</p>	
<p>8 Is the information publicly available?</p> <p>A) No - see Instructions below, then continue with Integrity questions B) Yes - see Instructions below, then continue with Integrity questions</p>	<p>8 Is the information (e.g., financial transactions, performance appraisals) relied upon to make business decisions? If yes, determine the impact of unauthorized modification or destruction of information.</p> <p>A) No - see Instructions below then continue with Availability questions B) Yes - Minimal impact - see Instructions below then continue with Availability questions. C) Yes - Limited impact - see Instructions below then continue with Availability questions. D) Yes - Severe impact - Integrity is High (rate below), continue with Availability questions.</p>	
<p>INSTRUCTIONS FOR RATING EACH COLUMN: IF ALL of the above answers are A/B (GREEN), rating is LOW; if ANY of the above answers are C (YELLOW) and NONE are D (RED), rating is MODERATE; if ANY of the above answers are D (RED), rating is HIGH SCALE: A/B = GREEN = LOW C = YELLOW = MODERATE D = RED = HIGH</p>		
CLASSIFICATION RATING FOR CONFIDENTIALITY: High	CLASSIFICATION RATING FOR INTEGRITY: Moderate	CLASSIFICATION RATING FOR AVAILABILITY: Low

HRM Form Classification Worksheet

Classifying the Information

Instructions for Rating Column

- You will have to answer most questions on a scale of no/none, minimal, limited, or severe
- If ALL of the column answers are A/B (GREEN), rating is LOW
- If ANY of the above answers are C (YELLOW) and NONE are D (RED), rating is MODERATE;
- If ANY of the above answers are D (RED), rating is HIGH
- SCALE:
 - A/B = GREEN = LOW
 - C = YELLOW = MODERATE
 - D = RED = HIGH

Classification Requirements

- Personal, Private or Sensitive Information (PPSI) must be classified with confidentiality of high
- If unable to determine the confidentiality classification, the asset must be classified with a confidentiality of high
- Information must be classified based on highest level necessitated by its individual data elements

Classification Requirements Cont'd.

- Merging of information which creates a new information asset or situation that creates the potential of merging (e.g., tape backup containing multiple files) requires re-evaluation of classification
- Full reproductions of information must carry the same confidentiality classification as original
 - Partial reproductions **MUST** be reviewed to see if re-classification is warranted

Storage & Review

- Information Classification Repository is needed
 - Important to document classification & store securely
 - Easier to manage centrally
 - Owner should be designated for repository
 - Must have high integrity
- Classification needs to be reviewed periodically because of
 - Obsolescence
 - Expiration/Changes in legislation
 - Change in SE mission

Validation

- The agency should assign a central unit to assist in ensuring consistency
- Legal issues may be referred to the appropriate legal staff for guidance
- Criteria for storage and disposal should be validated against agency's retention policy

Information Classification Process

Key Points

- Asset inventory forms basis for information classification
 - Information Asset Identification Worksheet
- Grouping of data may be done to make classification efficient
- Owner has responsibility for classification of data and making access decisions
- Information Classification Worksheet facilitates classification process
 - Manual should be used for help in classification

BREAK (15 min.)

EXERCISE 1

Part IV. Information Classification Controls

Controls

- Controls are safeguards that protect against damage caused by information security threats

- Purpose of controls is to:
 - Deter
 - Protect
 - Detect
 - Respond
 - Recover



Control Selection

- Selection of controls is a risk mitigation activity that either reduces, eliminates, or transfers risk of threats
- Control selection process involves
 - Identification of baseline security controls
 - Supplement baseline controls with additional controls based on needs of organization
 - Development, implementation, enforcement, & assessment of controls
 - Many controls should already be in place through compliance with NYS Information Security Policy P03-002

Source of CSCIC Baseline Controls

- Controls derived from work done in other standards bodies & government agencies
 - ISO 27002 (17799) (comprehensive security standard contains most control requirements)
 - ISO2700X (family of standards provides generally accepted practices on Information Security Management Systems)
 - NIST (multiple standards covering different aspects of security)
- Best Practices
 - Typically emerge from shared experience of multiple stakeholders

Control Charts

- Control charts contain baseline controls
 - 27 different control charts based on all possible information classification levels
- Control charts correspond to classification
 - e.g., for Confidentiality **Moderate**, Integrity **High**, & Availability **High**, use MHH control chart
 - Controls are cumulative***

	LHL	MHL	HHL		
	LHM	MHM	HHM		
	LHH	MHH	HHH		
LLL	MLL	HLL	LML	MML	HML
LLM	MLM	HLM	LMM	MLM	HLM
LLH	MLH	HLH	LMM	MLM	HLM

Classification Rating Menu (Appendix D)

- Excel workbook makes access to control charts easy
 - Index page allows us to select the right control chart
 - Glossary provides details of controls

Controls for each security dimension

Glossary

Control Chart Index

Page #	Classification Rating	Confidentiality	Integrity	Availability
1-	<u>LLL</u>	Low	Low	Low
2-	<u>LLM</u>	Low	Low	Moderate
3-	<u>LLH</u>	Low	Low	High
4-	<u>LML</u>	Low	Moderate	Low
5-	<u>LMM</u>	Low	Moderate	Moderate
6-	<u>LMH</u>	Low	Moderate	High
7-	<u>LHL</u>	Low	High	Low
8-	<u>LHM</u>	Low	High	Moderate
9-	<u>LHH</u>	Low	High	High
10-	<u>MLL</u>	Moderate	Low	Low
11-	<u>MLM</u>	Moderate	Low	Moderate
12-	<u>MLH</u>	Moderate	Low	High
13-	<u>MML</u>	Moderate	Moderate	Low
14-	<u>MMM</u>	Moderate	Moderate	Moderate
15-	<u>MMH</u>	Moderate	Moderate	High
16-	<u>MHL</u>	Moderate	High	Low
17-	<u>MHM</u>	Moderate	High	Moderate
18-	<u>MHH</u>	Moderate	High	High
19-	<u>HLL</u>	High	Low	Low
20-	<u>HLM</u>	High	Low	Moderate
21-	<u>HLH</u>	High	Low	High
22-	<u>HML</u>	High	Moderate	Low
23-	<u>HMM</u>	High	Moderate	Moderate
24-	<u>HMH</u>	High	Moderate	High
25-	<u>HHL</u>	High	High	Low
26-	<u>HHM</u>	High	High	Moderate
27-	<u>HHH</u>	High	High	High
28-	<u>Confidentiality Controls</u>			
29-	<u>Integrity Controls</u>			
30-	<u>Availability Controls</u>			
31-	<u>Glossary of Controls</u>			

Control Charts Sample

Security dimensions corresponding to control

Glossary Index Corresponding to Control

CONFIDENTIALITY (C): LOW		INTEGRITY (I): LOW	AVAILABILITY (A): LOW
Glossary X-Ref #	R=Required O=Optional		CIA
STATE ENTITY (SE) CONTROLS			
2	R Access approval/removal process in place		C
29	R Information classification and inventory		CIA
38	R Privacy disclaimer on e-mail and fax cover sheets		C
INFORMATION OWNER CONTROLS			
3	R Access authorized by information owner		C
43	R Review access lists		CI
45	R Review and reclassify information		CIA
INFORMATION CUSTODIAN CONTROLS			
12	R Basic input data validation		I
22	R Erase re-writeable media prior to reuse		C
25	O IAM Trust Level 1 for information systems		CI
55	R Use disposal method for re-writeable media		C
SE WORKFORCE (INFORMATION USER) CONTROLS			
31	O Label: "NYS CONFIDENTIALITY-LOW"		C
54	R Use disposal method for paper or write-once media		C
INFORMATION SECURITY OFFICER (ISO) CONTROLS			
46	R Review security procedures and controls		CIA

Controls are organized by **suggested** roles

Clicking on control will lead to corresponding glossary reference

Glossary (Appendix E)

- An alphabetic glossary of controls is provided along with control charts
 - All 27 classification ratings are hyperlinked to the appropriate control chart
 - Each control in control charts is hyperlinked to appropriate entry in glossary
 - Charts for each security dimension (CIA) are included in the Excel spreadsheet
 - ALT + LEFT ARROW keys to return to a previous page for ease of navigation in spreadsheet

Glossary Sample

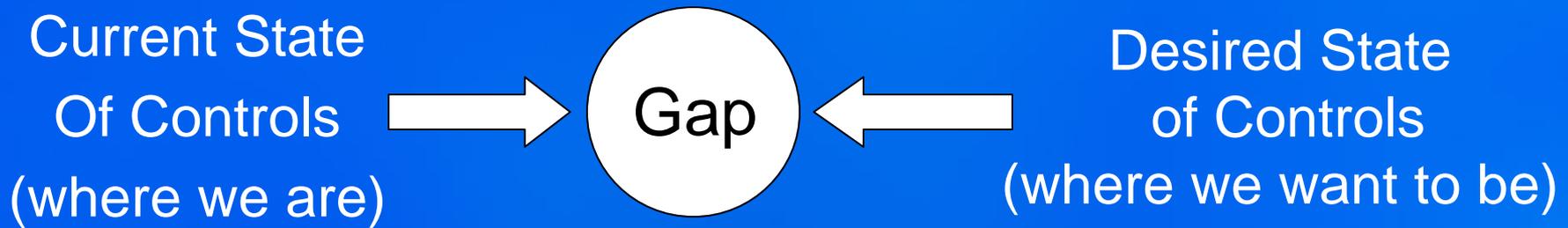
Some explanations have been truncated to fit on slide

#	CONTROL	NEED	CONTROL TYPE	EXPLANATION / CLARIFICATION	C I A	CONTROL RATING	SUGGESTED ROLE
1	Access approval/removal process (audit)	R	Authorization	Audit the access approval/removal process at least annually.	C	HIGH	ISO
2	Access approval/removal	R	Authorization	The SE must have a formal documented process in place to	C	LOW	SE
3	Access authorized by information owner	R	Authorization	Responsibility for authorizing access resides solely with the information owner. Users requiring access must follow SE's access approval process.	C	LOW	Owner
4	Access authorized by information owner (written)	R	Authorization	The information owner must provide written authorization for access. This does not include normal business processes such as IT having access to files for backup purposes or the travel unit having access to all employee travel documents. This authorizat	C	MODERATE	Owner
5	Access authorized by information owner (written & cc: exec)	R	Authorization	The information owner must provide written authorization for access with a cc: to executive management. This does not include normal business processes such as IT having access to files for backup purposes or the travel unit having access to all employe	C	HIGH	Owner

“HRM Form” Example Control Chart - HML

CONFIDENTIALITY (C): HIGH		INTEGRITY (I): MODERATE	AVAILABILITY (A): LOW
Glossary	R=Required O=Optional		CIA
X-Ref #			
STATE ENTITY (SE) CONTROLS			
2	R Access approval/removal process in place		C
9	R Approved electronic storage media and devices		C
10	R Approved storage facility		CI
13	R Chain of custody for physical media		C
17	R Destroy when no longer needed		C
23	R Formal change control procedures for information systems		I
24	R Formal test plans and documented results for information systems		I
29	R Information classification and inventory		CIA
36	R Non-Disclosure Agreement (NDA), Acceptable Use Policy, Memorandum of Understanding (MOU) or similar device for third-parties		C
38	R Privacy disclaimer on e-mail and fax cover sheets		C
40	R Reproduction authorized by information owner		C
48	R Review system and application security logs		CI
56	R Written approval for Transmission, Transportation and Storage (TTS)		C
INFORMATION OWNER CONTROLS			
5	R Access authorized by information owner (written & cc: exec)		C
44	R Review access lists (annually)		CI
45	R Review and reclassify information		CIA

Gap Analysis



Information owners should perform gap and work within their agency to ensure missing controls are implemented

Gap Analysis (State Entity)

STATE ENTITY (SE) CONTROLS		
2	R <u>Access approval/removal process in place</u>	✓
9	R <u>Approved electronic storage media and devices</u>	✓
10	R <u>Approved storage facility</u>	✓
13	R <u>Chain of custody for physical media</u>	✓
17	R <u>Destroy when no longer needed</u>	✓
23	R <u>Formal change control procedures for information systems</u>	✗
24	R <u>Formal test plans and documented results for information systems</u>	✓
29	R <u>Information classification and inventory</u>	✗
36	R <u>Non-Disclosure Agreement (NDA), Acceptable Use Policy, Memorandum</u>	✓
	R <u>similar device for third-parties</u>	✓
38	R <u>Privacy disclaimer on e-mail and fax cover sheets</u>	✗
40	R <u>Reproduction authorized by information owner</u>	✓
48	R <u>Review system and application security logs</u>	✗
56	R <u>Written approval for Transmission, Transportation and Storage (TTS)</u>	✗

Gap Analysis (Owner)

INFORMATION OWNER CONTROLS		
5	R <u>Access authorized by information owner (written & cc: exec)</u>	<input checked="" type="checkbox"/>
44	R <u>Review access lists (annually)</u>	<input checked="" type="checkbox"/>
45	R <u>Review and reclassify information</u>	<input type="checkbox"/>

Gap Analysis (Custodian)

INFORMATION CUSTODIAN CONTROLS		
11	R <u>Backup recovery procedures</u>	✓
12	R <u>Basic input data validation</u>	✓
16	R <u>Data plausibility and field comparison edits</u>	✗
18	R <u>Encryption for Transmission/ Transportation/ Storage (TTS) Outside the SE</u>	✓
19	R <u>Encryption/hashing of electronic authentication information</u>	✓
20	R <u>Environmental protection measures</u>	✓
22	R <u>Erase re-writeable media prior to reuse</u>	✓
27	R <u>IAM Trust Level 3 for information systems</u>	✓
28	O <u>IAM Trust Level 4 for information systems</u>	✗
33	R <u>Limit access to secure areas</u>	✗
39	R <u>Regular backup</u>	✓
55	R <u>Use disposal method for re-writeable media</u>	✓

Gap Analysis (Information User)

SE WORKFORCE (INFORMATION USER) CONTROLS			
15	R	Confirmation of identity and access rights of requester	✘
30	O	Label: "NYS CONFIDENTIALITY-HIGH"	✘
35	R	No confidential information in e-mail subject line	✔
41	R	Retrieval when printing/faxing (immediate)	✔
49	R	Secure area	✔
50	R	Secure physical media when unattended	✔
51	R	Situational awareness during verbal communications	✔
53	R	Transportation handling controls for paper	✔

Gap Analysis (ISO)

INFORMATION SECURITY OFFICER (ISO) CONTROLS		
1	R Access approval/removal process (audit) _	<input type="checkbox"/>
47	R Review security procedures and controls (annually) _	<input checked="" type="checkbox"/>

Exemption Process

- In case not able to comply with a baseline control, Exemption Request Form (Appendix A) should be filled out with:
 - Control to be exempted
 - Reasons for request
 - Risks posed by lack of control
 - Compensating controls (if any)
- Approval needed by:
 - Information Owner / Business Manager
 - ISO/CIO
 - Executive Management

 NEW YORK STATE OFFICE OF CYBER SECURITY & CRITICAL INFRASTRUCTURE COORDINATION Information Classification and Control Standard Exemption Request		
Section 1: Exemption Description		
1.1 Requestor Information		
Name:	Phone:	Date:
Agency/Division:	E-mail:	
1.2 Exemption Details		
Control Number:		
Control Name:		
Exemption Review Date (re-authorization will be required minimally once a year):		
System(s)/ Hardware Impacted:	Will this impact the processing/ storage/ transmission of PPSI?	<input type="checkbox"/> Yes <input type="checkbox"/> No
1.3 Reason for Exemption Request: List constraints precluding compliance with the control		
1.4 Description of Risk(s): Identify risk(s) posed by the lack of the original control		
1.5 Compensating Control(s): List the compensating control(s) and explain how they address the objectives of the original control		
1.6 Approval by Information Owner/Business Manager	Name/Signature:	Date:
Section 2: Executive Authorization		
2.1 Information Security Officer	Name/Signature:	Date:
2.2 Chief Information Officer	Name/Signature:	Date:
2.3 Commissioner/Executive Deputy Commissioner or equivalent	Name/Signature:	Date:
Please mail to 30 South Pearl St. P2 Albany, NY 12207 or fax to (518) 402-3799.		
<small>NYS Confidentiality-High V1.0 October 10, 2008 Page 1 of 1</small>		

Information Classification Controls

Key Points

- Controls are deployed to reduce the chance of damage caused by threats
 - Has been simplified through use of control charts
- Baseline controls are provided
 - Supplemental controls may be added by SE
 - Control exemptions should be documented

Part V. How Does an Agency Begin?

Buy-In

- Information classification requires support of the entire organization
- Security is everyone's business
- Create a business case based on
 - Benefits of protection
 - Impact of legislation (e.g., SOX, HIPAA)
 - Cost of implementation

Creating the Team

- Select team members that have a good understanding of the business processes and data used in the process
- Consider different skill sets while creating a team, e.g., technical, business, management
- Goal of the team is to facilitate the decision making of the data owners
 - If owners have to make decisions about access they need to understand the classification rationale

Find a Committed Business Unit

- Initial success is very critical for rolling out the complete information classification program
- Select a small/medium size unit in the organization
 - Understand that it will be a collaborative effort
 - Will require resources to be assigned
 - Should have a champion within the unit
- Assume a strong mentoring role for the first case
- Create Best Practices & FAQ
 - Update them based on experience

After Initial Roll-out

- Focus on top 5 critical business functions
- Ensure that all Internet applications are compliant with the Information Classification Policy
- Ensure that any new applications are compliant right from the beginning

Information Classification

Wrap-up

- Information classification is the first step towards managing security risks
- CSCIC has provided a comprehensive toolset to classify information and select baseline controls
 - Familiarize yourself with the CSCIC information classification materials
 - Available at www.cscic.state.ny.us/lib/policies/
- Contact your ISO and other Subject Matter Experts within your agency for assistance