Protecting Information Assets
- Week 3 -

Data Classification Processes and Models
MIS5206 Week 3

• Readings
• In the News
• Data Classification Processes and Models
• Test Taking Tip
• Quiz
Readings


• FIPS Reading 1: “Standards for Security Categorization of Federal Information and Information Systems”

• FGDC Reading 1: “Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns”

• ISO 27001 – Reading 1: ISO 27001 Data Security Classifications Model Policy
In the News

US 911 emergency phone system vulnerable to DDoS Attacks, say researchers

“Researchers...using a telephony denial-of-service (TDoS) attack targeting 911 call centres....

...a hacker could cause mobile phones to call 911 automatically without a user’s knowledge, essentially clogging up the PSAP’s (public safety answering points) queues and preventing legitimate callers from reaching the service. ...

Federal Communications Commission (FCC) regulations stipulate that wireless carriers must forward all 911 calls to a PSAP, regardless of caller validation, giving a malicious hacker the perfect opportunity to exploit this ruling with an anonymized form of a distribute denial of service (DDoS) attack.

By placing a rootkit within a baseband firmware of a mobile phone, a hacker can mask and randomize a mobile phone’s identifiers, essentially resulting in a device that has no identity in the cellular network.”

http://www.ibtimes.co.uk/us-911-emergency-phone-system-vulnerable-ddos-attacks-say-researchers-1580674
Last week – Threats, Vulnerabilities, Risks, and Risk mitigations

- Risk Mitigation Controls – *your answers*
  - Preventative
  - Detective
  - Corrective

<table>
<thead>
<tr>
<th>Preventative</th>
<th>Detective</th>
<th>Corrective</th>
<th>Compensatory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Awareness Training</td>
<td>System Monitoring</td>
<td>OS Upgrade</td>
<td>Backup Generator</td>
</tr>
<tr>
<td>Firewall</td>
<td>IDS</td>
<td>Backup Data Restoral</td>
<td>Hot Site</td>
</tr>
<tr>
<td>Anti-virus</td>
<td>Anti-Virus</td>
<td>Anti-Virus</td>
<td>Server Isolation</td>
</tr>
<tr>
<td>Security Guard</td>
<td>Motion Detector</td>
<td>Vulnerability Mitigation</td>
<td></td>
</tr>
<tr>
<td>IPS</td>
<td>IPS</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

These are sometimes referred to as “*phase controls*”

http://www.sans.edu/research/security-laboratory/article/security-controls
Last week – Threats, Vulnerabilities, Risks, and Risk mitigations

• Risk Mitigation Controls – from our Vacca reading...
  – Physical
  – Technical
  – Administrative

Administrative is the most important!

Way to go Priya and Binu!
Projected Growth of Data

The Digital Universe in the Clouds, 2020

By 2020, more than a third of the Digital Universe will either live in or pass through the cloud

Total Digital Universe: 35 ZB

Touched by Cloud: 12 ZB

Source: IDC Digital Universe Study, sponsored by EMC, May 2010
© Copyright 2010 EMC Corporation. All rights reserved.
# Projected Growth of Data

## What is a Zetta Byte?

A zettabyte is a quantity of information or information storage capacity equal to $10^{21}$ bytes.

Research from the University of California, San Diego reports that in 2008, Americans consumed 3.6 zettabytes of information.

<table>
<thead>
<tr>
<th>Processor or Virtual Storage</th>
<th>Disk Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Bit = Binary Digit</td>
<td>1 Bit = Binary Digit</td>
</tr>
<tr>
<td>8 Bits = 1 Byte</td>
<td>8 Bits = 1 Byte</td>
</tr>
<tr>
<td>1024 Bytes = 1 Kilobyte</td>
<td>1000 Bytes = 1 Kilobyte</td>
</tr>
<tr>
<td>1024 Kilobytes = 1 Megabyte</td>
<td>1000 Kilobytes = 1 Megabyte</td>
</tr>
<tr>
<td>1024 Megabytes = 1 Gigabyte</td>
<td>1000 Megabytes = 1 Gigabyte</td>
</tr>
<tr>
<td>1024 Gigabytes = 1 Terabyte</td>
<td>1000 Gigabytes = 1 Terabyte</td>
</tr>
<tr>
<td>1024 Terabytes = 1 Petabyte</td>
<td>1000 Terabytes = 1 Petabyte</td>
</tr>
<tr>
<td>1024 Petabytes = 1 Exabyte</td>
<td>1000 Petabytes = 1 Exabyte</td>
</tr>
<tr>
<td>1024 Exabytes = 1 Zettabyte</td>
<td>1000 Exabytes = 1 Zettabyte</td>
</tr>
<tr>
<td>1024 Zettabytes = 1 Yottabyte</td>
<td>1000 Zettabytes = 1 Yottabyte</td>
</tr>
<tr>
<td>1024 Yottabytes = 1 Brontobyte</td>
<td>1000 Yottabytes = 1 Brontobyte</td>
</tr>
<tr>
<td>1024 Brontobytes = 1 Geopbyte</td>
<td>1000 Brontobytes = 1 Geopbyte</td>
</tr>
</tbody>
</table>

This is based on the IBM Dictionary of computing method to describe storage - the simplest.
Projected Growth of Data

The Crisis in IT Management

From 2009 to 2020...

The number of information containers – files, packets, images – (what is actually managed, protected, and stored in the Digital Universe) will grow 67 times.

The amount of information will grow 44 times.

But the number of IT professionals in the world will grow only 1.4 times.

© Copyright 2010 EMC Corporation. All rights reserved.

MIS 5206 Protecting Information Assets
Projected Growth of Data

The Decreasing Cost of Managing Information will be an Incentive to Create More Information

Total Investment in the Digital Universe: $4 Trillion in 2009

Investment per Gigabyte

Zettabytes

Source: IDC Digital Universe Study, sponsored by EMC, May 2010
© Copyright 2010 EMC Corporation. All rights reserved.

MIS 5206 Protecting Information Assets
Projected Growth of Data

Unprotected Data Needing Protection

Source: IDC Digital Universe Study, sponsored by EMC, May 2010; chart does not include data that does not need protection

© Copyright 2010 EMC Corporation. All rights reserved.
Key Concepts

Classification
Grouping of data according to pre-determined types

Cost-Effectiveness
Appropriateness of the level of risk mitigation expenditure

Confidentiality
Restriction who may know about and/or have access to information

Integrity
Confidence that information is complete and unaltered

Availability
Access to information
Data classification is essential to ensuring that data is appropriately protected and done so in the most cost-effective manner.

The goal is to classify data according to its risk associated with its loss or disclosure and to identify the level of confidentiality, integrity and availability required.
MIS 5206 Protecting Information Assets

1946
The First Satellite Design

More than 11 years before Sputnik, RAND released its first report while still at Douglas Aircraft, Preliminary Design of an Experimental World-Circling Spaceship. At the time, it was the most comprehensive engineering study of the nuts-and-bolts realities of a satellite spacecraft.

1948
The JOHNNIAC

When the need for solutions to complex analytic studies outstripped the computing power of the time, RAND decided to build its own computer. Named after mathematician John von Neumann, the JOHNNIAC was one of the first mainframe computers with stored memory.

1954
Selection and Use of Strategic Air Bases

The report by a team led by Albert Wohlstetter shook the foundation of nuclear deterrence policy by shifting the United States from a first-strike to a second-strike posture. It suggested placing air bases closer to the United States and relying on long-range bombers and aerial refueling aircraft, eventually saving the Air Force billions of dollars.

1957
Artificial Intelligence

The first successful Artificial Intelligence program that used Information Processing Languages (IPLs) was developed in RAND's Systems Research Laboratory. IPLs were the precursors of popular contemporary languages such as LISP.

1961
The RAND Tablet

The tablet was one of the first devices permitting the input of handwritten text and freehand drawings into a computer. While limited in its capabilities and far too expensive for commercial use, the RAND Tablet nonetheless showed the way for Palm Pilots, Tablet PCs, and iPads.

1962
Packet Switching: Seed of the Internet

Paul Baran developed a plan for a communication network that would withstand a nuclear attack. This notion of distributed communications, or packet switching, eventually became the foundation of the Internet.

1974
Improving Computer Security

RAND's expertise in defense-related computer security issues was extended to the private sector during the 1970s. Willis Ware chaired a government committee that studied the problems arising from the application of computer technology to record keeping about people. This work guided the DoD computer configurations and eventually became the foundation of the Federal Privacy Act of 1974.
Risks from public geospatial information

In 2003, Director of U.S. National Imagery and Mapping Agency asked RAND Corporation for a:

Framework to “guide public and private decision makers in weighing homeland security implications related to release of geospatial information”

Today the National Imagery and Mapping Agency is called the National Geospatial-Intelligence Agency

http://www.rand.org/about/history.html
Risks from public geospatial information

RAND’s 2004 deliverable included a survey and analysis of

- 465 programs/offices/initiatives at 30 agencies and departments identified as providing geospatial information to the public
  - 628 public datasets sampled from NSDI Clearinghouse websites
  - 37 (~6%) found to be useful in helping an attacker select a target or plan an attack against a site
    - None were considered so critical that an “attacker could not perform the attack without” them

- Conclusions
  - Publicly available geospatial “information needed for identifying and locating potential targets is widely accessible”
  - “…detailed and up-to-date information required for attack planning against a particular target is much less readily available”
RAND’s assessment of risks posed by GIS data shared publicly over the Internet is focused by 3 “filters”

<table>
<thead>
<tr>
<th>Filter</th>
<th>Key Questions for Decisionmakers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Usefulness</td>
<td>• Is the information useful for target selection or location purposes?</td>
</tr>
<tr>
<td></td>
<td>• Is the information useful for attack planning purposes?</td>
</tr>
<tr>
<td>Uniqueness</td>
<td>• Is the information readily available from other geospatial information sources?</td>
</tr>
<tr>
<td></td>
<td>• Is the information available from direct observation or other nongeospatial information types?</td>
</tr>
<tr>
<td>Societal benefits and costs</td>
<td>• What are the expected security benefits of restricting public access to the source?</td>
</tr>
<tr>
<td></td>
<td>• What are the expected societal costs of restricting public access to the source?</td>
</tr>
</tbody>
</table>
Federal Geographic Data Committee’s risk assessment and control guidelines for...

- Identifying sensitive information contents of geospatial data that pose a risk to security
- Making information security decisions and applying safeguards to sensitive geospatial data contents

“Does knowledge of the location and purpose of a feature as described in the data, have the potential to significantly compromise the security of persons, property, or systems?”

FGDC 2005, based on RAND’s 2004 study
Figure 1. Decision Tree for Providing Appropriate Access to Geospatial Data in Response to Security Concerns

1. Did your organization originate these data?
   Yes
   2. Follow instructions of originating organization
   No

3. Document your use of the decision procedure.
   (Have the sensitivity concerns been addressed by the changes to data?)

4. Are these data useful for selecting specific target(s), and/or for planning and executing an attack on a potential target?
   Yes
   7. Safeguarding is not justified.
   No

5. Is the information unique to these data?
   Yes
   No

6. Do the security costs outweigh the societal benefits of active dissemination of these data?
   Yes
   No

8. Would the public still be served, and the security risk be mitigated, by changing these data?
   Yes
   10. Change these data.
   No

9. Do you have the authority to change these data?
   Yes
   12. Will the appropriate decision maker give permission to restrict these data?
   No

10. Decide the extent of restrictions.
   Yes
   Safeguarding is not authorized.
   No

Guidelines for Providing Appropriate Access to Geospatial Data in Response to Security Concerns

MIS 5206 Protecting Information Assets
Decision Tree for Providing Appropriate Access to Geospatial Data in Response to Security Concerns

Section 1: Is it your decision to apply safeguards to these data?

1. Did your organization originate these data?
   Yes
   3. Document your use of the decision procedure.
   No
   2. Follow instructions of originating organization
“Sensitivity” of geospatial data is based on usefulness to terrorists.

Do the data show “choke points to increase effectiveness of an attack?”
Do the data “provide relevant current (real-time, near real-time, or very recent) security-related data” that can help an attacker “find the best way to cause catastrophic failure”?

“Sensitivity” of geospatial data is based on usefulness to terrorists.
Assess the risk...

4. Are these data useful for selecting specific target(s), and/or for planning and executing an attack on a potential target?

Yes → 5. Is the information unique to these data?

Yes → 6. Do the security costs outweigh the societal benefits of active dissemination of these data?

Yes → 7. Safeguarding is not justified.

No → 6. Do the security costs outweigh the societal benefits of active dissemination of these data?

No → 5. Is the information unique to these data?

No → 7. Safeguarding is not justified.

No → 4. Are these data useful for selecting specific target(s), and/or for planning and executing an attack on a potential target?
...control/mitigate the risk...

4. Are these data useful for selecting specific target(s), and/or for planning and executing an attack on a potential target?

Yes

5. Is the information unique to these data?

Yes

6. Do the security costs outweigh the societal benefits of active dissemination of these data?

Yes

8. Would the public still be served, and the security risk be mitigated, by changing these data?

Yes → 9. Do you have the authority to change these data?

Yes → 10. Change these data.

No → 7. Safeguarding is not justified.

No

No

No
...control/mitigate the risk...

8. Would the public still be served, and the security risk be mitigated, by changing these data?

- Yes
  - 9. Do you have the authority to change these data?
    - Yes: 10. Change these data.
    - No: 11. Do you have the authority to restrict these data?
      - No: 12. Will the appropriate decision maker give permission to restrict these data?
        - Yes: 14. Safeguarding is not authorized.
        - No: No

Section III: What safeguards are authorized and justified?

11. Do you have the authority to restrict these data?

- Yes
- No

12. Will the appropriate decision maker give permission to restrict these data?

- Yes
- No
If security risks outweigh benefits of releasing the data to the public, agency can choose to safeguard data by:

- **Modifying data**
  - Remove or reduce detail in offending data elements
    - either in the attributes, spatial representations, or both

- **Restricting access to data**
  - If agency lacks authority to change data, or believes modifying data will undermine its value to the public, then agency can restrict access
To remove or reduce detail in offending data elements apply techniques of **Cartographic Generalization**

1. **Selective Omission**
2. **Simplification**
3. **Combination**
4. **Exaggeration**
5. **Displacement**

...control/mitigate risk...

Before... ...after
Figure 1. Decision Tree for Providing Appropriate Access to Geospatial Data in Response to Security Concerns

1. Did your organization originate these data?
   - Yes
   - No

2. Follow instructions of originating organization

3. Document your use of the decision procedure.

4. Are these data useful for selecting specific target(s), and/or for planning and executing an attack on a potential target?
   - Yes
   - No

5. Is the information unique to these data?
   - Yes
   - No

6. Do the security costs outweigh the societal benefits of active dissemination of these data?
   - Yes
   - No

7. Safeguarding is not justified.

8. Would the public still be served, and the security risk be mitigated, by changing these data?
   - Yes
   - No

9. Do you have the authority to change these data?
   - Yes
   - No

10. Change these data.

11. Do you have the authority to restrict these data?
   - Yes
   - No

12. Will the appropriate decision maker give permission to restrict these data?
   - Yes
   - No

13. Decide the extent of restrictions.

14. Safeguarding is not authorized.

...but this time with...
Metadata standards for documenting geospatial datasets
Decision Tree for Providing Appropriate Access to Geospatial Data in Response to Security Concerns

1. Did your organization originate these data?  
   Yes  
   3. Document your use of the decision procedure.  
   No  
   Follow instructions of originating organization

Section I: Is it your decision to apply safeguards to these data?
Appendix 2: Documenting Use of the Guidelines in Metadata Accompanying Geospatial Data

This appendix identifies data elements in the “Content Standard for Digital Geospatial Metadata” (Federal Geographic Data Committee, 1998) that are available for documenting the use of the guidelines in the metadata.

Four types of information should be encoded in metadata:

1. The fact that the geospatial data and metadata were reviewed using the guidelines.
2. Decisions that were made.
3. The date of the decisions.
4. The safeguards (changes to the geospatial data or restrictions on access, use, or dissemination of the geospatial data and metadata) that were applied.

If your organization has a formal classification system you also can report the classification level of the geospatial data by category under “Security Information” (element 1.12).

Geospatial metadata can also be subject to safeguarding. To document the details of restrictions on access, use, or dissemination of the metadata:

- Report restrictions on access to the geospatial metadata under “Metadata Access Constraints” (element 7.8).

Document your use of the decision procedure.
3. Document your use of the decision procedure.

Four types of information should be encoded in metadata: (1) the fact that the geospatial data and metadata were reviewed using the guidelines, (2) decisions that were made, (3) the date of the decisions, and (4) the safeguards (changes to the geospatial data or restrictions on access, use, or dissemination of the geospatial data and metadata) that were applied.
3. Document your use of the decision procedure.

Four types of information should be encoded in metadata: (1) the fact that the geospatial data and metadata were reviewed using the guidelines, (2) decisions that were made, (3) the date of the decisions, and (4) the safeguards (changes to the geospatial data or restrictions on access, use, or dissemination of the geospatial data and metadata) that were applied.
Section 1
Identification Information

1.1 Citation Information
- Citation Information (see section 9)
  - Time Period of Content
  - Time Period Information (see section 9)
  - Currentness Reference

1.1.2 Description
- Abstract
- Purpose
- Supplemental Information

1.3 Status
- Progress
- Maintenance and Update Frequency

1.4 Spatial Domain
- Bounding Coordinate
  - West Bounding Coordinate
  - East Bounding Coordinate
  - North Bounding Coordinate
  - South Bounding Coordinate

1.5 Data Set G-Polygon
- (can be repeated unlimited times)
  - G-Ring Point
    - (4 to an unlimited number of repetitions)
    - G-Ring Latitude
    - G-Ring Longitude
  - Of
    - G-Ring

1.6 Keywords
- Theme
  - (can be repeated unlimited times)
- Theme Keyword Thesaurus

1.7 Place
- Place
  - (can be repeated unlimited times)
- Place Keyword
  - (can be repeated unlimited times)

1.8 Use Constraints

1.9 Security Information
- Security Classification System
- Security Classification
- Security Handling Description
- Security Information

1.10 Point of Contact
- Data Set Credit
- Native Data Set Environment

1.11 Cross Reference
- (can be repeated unlimited times)

1.12 Browse Graphic
- (can be repeated unlimited times)

1.13 Browse Graphic File Name
- Browse Graphic File Description
- Browse Graphic File Type

1.14 Browse Graphic File

Legend:
- mandatory
- optional
- 3-D box indicates near firey field


13. Decide the extent of restrictions.
3. Document your use of the decision procedure.

Four types of information should be encoded in metadata: (1) the fact that the geospatial data and metadata were reviewed using the guidelines, (2) decisions that were made, (3) the date of the decisions, and (4) the safeguards (changes to the geospatial data or restrictions on access, use, or dissemination of the geospatial data and metadata) that were applied.
Cartographic Generalization

1. Selective Omission
2. Simplification
3. Combination
4. Exaggeration
5. Displacement

Before... …after
Most FGDC Metadata are “unstructured”

1.7 Access Constraints -- restrictions and legal prerequisites for accessing the data set. These include any access constraints applied to assure the protection of privacy or intellectual property, and any special restrictions or limitations on obtaining the data set.
   Type: text
   Domain: "None" free text
   Short Name: accconst

1.8 Use Constraints -- restrictions and legal prerequisites for using the data set after access is granted. These include any use constraints applied to assure the protection of privacy or intellectual property, and any special restrictions or limitations on using the data set.
   Type: text
   Domain: "None" free text
   Short Name: useconst

1.12 Security Information -- handling restrictions imposed on the data set because of national security, privacy, or other concerns.
   Type: compound
   Short Name: secinfo

1.12.1 Security Classification System -- name of the classification system.
   Type: text
   Domain: free text
   Short Name: seccsys

1.12.2 Security Classification -- name of the handling restrictions on the data set.
   Type: text
   Domain: "Top secret" "Secret" "Confidential" "Restricted" "Unclassified" "Sensitive" free text
   Short Name: soclass

1.12.3 Security Handling Description -- additional information about the restrictions on handling the data set.
   Type: text
   Domain: free text
   Short Name: sechandl
...security classification for geospatial data...

1.12 Security Information -- handling restrictions imposed on the data set because of national security, privacy, or other concerns.
   Type: compound
   Short Name: secinfo

   1.12.1 Security Classification System -- name of the classification system.
       Type: text
       Domain: free text
       Short Name: secsys

   1.12.2 Security Classification -- name of the handling restrictions on the data set.
       Type: text
       Domain: "Top secret" "Secret" "Confidential" "Restricted" "Unclassified" "Sensitive" free text
       Short Name: secclass

   1.12.3 Security Handling Description -- additional information about the restrictions on handling the data set.
       Type: text
       Domain: free text
       Short Name: sechandl
ISO 19115-1 Geospatial metadata standard

**MD_SecurityConstraints**
- **classification**: MD_ClassificationCode
- **userNote**: CharacterString [0..1]
- **classificationSystem**: CharacterString [0..1]
- **handlingDescription**: CharacterString [0..1]

**MD_Releasability**
- **addressee**: CI_Responsibility [0..*]
- **statement**: CharacterString [0..1]
- **disseminationConstraints**: MD_RestrictionCode [0..1]

{count (addressee + statement) > 0}
Department of Defense’ Information Assurance (IA)

...also categorizes information systems and data in terms of CIA...

### Confidentiality Levels

<table>
<thead>
<tr>
<th>LEVEL</th>
<th>DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Classified Information</td>
</tr>
<tr>
<td>Medium</td>
<td>Sensitive Information, Not Cleared for Public Release</td>
</tr>
<tr>
<td>Basic</td>
<td>Information Cleared for Public Release</td>
</tr>
</tbody>
</table>

### Mission Assurance Categories

- **MAC I** — vital to operational readiness or mission effectiveness of deployed or contingency forces. Loss of integrity or availability unacceptable. Requires most stringent protective measures.

- **MAC II** — important to the support of deployed or contingency forces. Loss of integrity unacceptable, unavailability tolerable only for short time. Require additional safeguards beyond best practices.

- **MAC III** — necessary to conduct of day-to-day business. Protection commensurate with commercial best practices.

---

MIS 5206 Protecting Information Assets
Federal Information Processing Standards (FIPS) Security Categorization Standards

FIPS PUB 199

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Standards for Security Categorization of Federal Information and Information Systems

February 2004
Categorization is based on security objectives...

**Confidentiality**
Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

**Integrity**
Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

**Availability**
Ensuring timely and reliable access to and use of information.

MIS 5206 Protecting Information Assets
What are the security objective(s) of FGDC’s Guidelines?

**Confidentiality**
Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

**Integrity**
Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

**Availability**
Ensuring timely and reliable access to and use of information.
FIPS 199’s and FGDC Guidelines’ share a mutual security objective...

Confidentiality
Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Integrity
Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

Availability
Ensuring timely and reliable access to and use of information.

FGDC Guidelines’ security objective
FIPS 199’s and FGDC Guidelines’ share a mutual security objective...

Confidentiality
Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Integrity
Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

Availability
Ensuring timely and reliable access to and use of information.

FGDC Guidelines’ security objective
<table>
<thead>
<tr>
<th>Security Objective</th>
<th>LOW</th>
<th>MODERATE</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Confidentiality</strong></td>
<td>The unauthorized disclosure of information could be expected to have a <strong>limited</strong> adverse effect on organizational operations, organizational assets, or individuals.</td>
<td>The unauthorized disclosure of information could be expected to have a <strong>serious</strong> adverse effect on organizational operations, organizational assets, or individuals.</td>
<td>The unauthorized disclosure of information could be expected to have a <strong>severe or catastrophic</strong> adverse effect on organizational operations, organizational assets, or individuals.</td>
</tr>
</tbody>
</table>

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

[44 U.S.C., SEC. 3542]
### Standards for Security Categorization of Federal Information and Information Systems

<table>
<thead>
<tr>
<th>Security Objective</th>
<th>LOW</th>
<th>MODERATE</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Integrity</strong></td>
<td>The unauthorized modification or destruction of information could be expected to have a <strong>limited</strong> adverse effect on organizational operations, organizational assets, or individuals.</td>
<td>The unauthorized modification or destruction of information could be expected to have a <strong>serious</strong> adverse effect on organizational operations, organizational assets, or individuals.</td>
<td>The unauthorized modification or destruction of information could be expected to have a <strong>severe or catastrophic</strong> adverse effect on organizational operations, organizational assets, or individuals.</td>
</tr>
</tbody>
</table>

Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

[44 U.S.C., SEC. 3542]
<table>
<thead>
<tr>
<th>Security Objective</th>
<th>POTENTIAL IMPACT</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Availability</strong></td>
<td>LOW</td>
</tr>
<tr>
<td>Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]</td>
<td>The disruption of access to or use of information or an information system could be expected to have a <strong>limited</strong> adverse effect on organizational operations, organizational assets, or individuals.</td>
</tr>
<tr>
<td></td>
<td>MODERATE</td>
</tr>
<tr>
<td></td>
<td>The disruption of access to or use of information or an information system could be expected to have a <strong>serious</strong> adverse effect on organizational operations, organizational assets, or individuals.</td>
</tr>
<tr>
<td></td>
<td>HIGH</td>
</tr>
<tr>
<td></td>
<td>The disruption of access to or use of information or an information system could be expected to have a <strong>severe or catastrophic</strong> adverse effect on organizational operations, organizational assets, or individuals.</td>
</tr>
</tbody>
</table>
FIPS 199: Security objectives and impact ratings

**Low:** Limited adverse effect

**Moderate:** Serious adverse effect

**High:** Severe or catastrophic adverse effect

<table>
<thead>
<tr>
<th>Security Objective</th>
<th>LOW</th>
<th>MODERATE</th>
<th>HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>The unauthorized disclosure of information could be expected to have a <strong>limited</strong> adverse effect on organizational operations, organizational assets, or individuals.</td>
<td>The unauthorized disclosure of information could be expected to have a <strong>serious</strong> adverse effect on organizational operations, organizational assets, or individuals.</td>
<td>The unauthorized disclosure of information could be expected to have a <strong>severe</strong> or <strong>catastrophic</strong> adverse effect on organizational operations, organizational assets, or individuals.</td>
</tr>
<tr>
<td>Integrity</td>
<td>The unauthorized modification or destruction of information could be expected to have a <strong>limited</strong> adverse effect on organizational operations, organizational assets, or individuals.</td>
<td>The unauthorized modification or destruction of information could be expected to have a <strong>serious</strong> adverse effect on organizational operations, organizational assets, or individuals.</td>
<td>The unauthorized modification or destruction of information could be expected to have a <strong>severe</strong> or <strong>catastrophic</strong> adverse effect on organizational operations, organizational assets, or individuals.</td>
</tr>
<tr>
<td>Availability</td>
<td>The disruption of access to or use of information or an information system could be expected to have a <strong>limited</strong> adverse effect on organizational operations, organizational assets, or individuals.</td>
<td>The disruption of access to or use of information or an information system could be expected to have a <strong>serious</strong> adverse effect on organizational operations, organizational assets, or individuals.</td>
<td>The disruption of access to or use of information or an information system could be expected to have a <strong>severe</strong> or <strong>catastrophic</strong> adverse effect on organizational operations, organizational assets, or individuals.</td>
</tr>
</tbody>
</table>
FIPS Pub 199 Standards for Security Categorization of Federal Information and Information Systems

Low: Limited adverse effect
Medium: Serious adverse effect
High: Severe or catastrophic adverse effect

The generalized format for expressing the security category, SC, of an information system is:

\[ SC \text{ information system} = \{(\text{confidentiality, impact}), (\text{integrity, impact}), (\text{availability, impact})\}, \]

where the acceptable values for potential impact are LOW, MODERATE, or HIGH.

Example with multiple information types:

\[ SC \text{ contract information} = \{(\text{confidentiality, MODERATE}), (\text{integrity, MODERATE}), (\text{availability, LOW})\}, \]

and

\[ SC \text{ administrative information} = \{(\text{confidentiality, LOW}), (\text{integrity, LOW}), (\text{availability, LOW})\}. \]

The resulting security category of the information system is expressed as:

\[ SC \text{ acquisition system} = \{(\text{confidentiality, MODERATE}), (\text{integrity, MODERATE}), (\text{availability, LOW})\}, \]
There are alternative “code word” classification systems for data

The need to protect information is different in different sorts of organizations

A principal distinction exists between Government and Business

But, the terms used for CUI overlap in scope and are often intermingled often resulting in confusion
# U.S. Federal Government Classification Levels

<table>
<thead>
<tr>
<th>Clearance</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Highest</td>
<td>Top secret</td>
<td>Unauthorized disclosure could be expected to cause “exceptionally grave damage” to national security</td>
</tr>
<tr>
<td>2nd highest</td>
<td>Secret</td>
<td>Unauthorized disclosure would cause “serious damage” to national security</td>
</tr>
<tr>
<td>Lowest</td>
<td>Confidential</td>
<td>Unauthorized disclosure would “damage” national security</td>
</tr>
<tr>
<td>Unclassified</td>
<td>Sensitive But Classified</td>
<td>Synonym</td>
</tr>
<tr>
<td>Unclassified</td>
<td>For Official Use Only (FOUO)</td>
<td>Synonym</td>
</tr>
<tr>
<td>Controlled</td>
<td>Controlled Unclassified</td>
<td>Synonym</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

*MIS 5206 Protecting Information Assets*
A traditional business-oriented information security classification system...

<table>
<thead>
<tr>
<th>Information Category</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unclassified Public</td>
<td>Information is not confidential and can be made public without any implications for Company. Loss of availability due to system downtime is an acceptable risk. Integrity is important but not vital.</td>
<td>• Product brochures widely distributed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Information widely available in the public domain, including publicly available Company web site areas</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Sample downloads of Company software that is for sale</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Financial reports required by regulatory authorities</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Newsletters for external transmission</td>
</tr>
<tr>
<td>Proprietary</td>
<td>Information is restricted to management-approved internal access and protected from external access. Unauthorized access could influence Company’s operational effectiveness, cause an important financial loss, provide a significant gain to a competitor, or cause a major drop in customer confidence. Information integrity is vital.</td>
<td>• Passwords and information on corporate security procedures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Know-how used to process client information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Standard Operating Procedures used in all parts of Company’s business</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• All Company-developed software code, whether used internally or sold to clients</td>
</tr>
<tr>
<td>Client Confidential Data</td>
<td>Information received from clients in any form for processing in production by Company. The original copy of such information must not be changed in any way without written permission from the client. The highest possible levels of integrity, confidentiality, and restricted availability are vital.</td>
<td>• Client media</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Electronic transmissions from clients</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Product information generated for the client by Company production activities as specified by the client</td>
</tr>
<tr>
<td>Company Confidential Data</td>
<td>Information collected and used by Company in the conduct of its business to employ people, to log and fulfill client orders, and to manage all aspects of corporate finance. Access to this information is very restricted within the company. The highest possible levels of integrity, confidentiality, and restricted availability are vital.</td>
<td>• Salaries and other personnel data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Accounting data and internal financial reports</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Confidential customer business data and confidential contracts</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Non disclosure agreements with clients/vendors</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Company business plans</td>
</tr>
</tbody>
</table>
Which of these would be considered CUI?

<table>
<thead>
<tr>
<th>Information Category</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
</table>
| Unclassified Public  | Information is not confidential and can be made public without any implications for Company. Loss of availability due to system downtime is an acceptable risk. Integrity is important but not vital. | • Product brochures widely distributed  
• Information widely available in the public domain, including publicly available Company web site areas  
• Sample downloads of Company software that is for sale  
• Financial reports required by regulatory authorities  
• Newsletters for external transmission |
| Proprietary          | Information is restricted to management-approved internal access and protected from external access. Unauthorized access could influence Company’s operational effectiveness, cause an important financial loss, provide a significant gain to a competitor, or cause a major drop in customer confidence. Information integrity is vital. | • Passwords and information on corporate security procedures  
• Know-how used to process client information  
• Standard Operating Procedures used in all parts of Company’s business  
• All Company-developed software code, whether used internally or sold to clients |
| Client Confidential Data | Information received from clients in any form for processing in production by Company. The original copy of such information must not be changed in any way without written permission from the client. The highest possible levels of integrity, confidentiality, and restricted availability are vital. | • Client media  
• Electronic transmissions from clients  
• Product information generated for the client by Company production activities as specified by the client |
| Company Confidential Data | Information collected and used by Company in the conduct of its business to employ people, to log and fulfill client orders, and to manage all aspects of corporate finance. Access to this information is very restricted within the company. The highest possible levels of integrity, confidentiality, and restricted availability are vital. | • Salaries and other personnel data  
• Accounting data and internal financial reports  
• Confidential customer business data and confidential contracts  
• Non disclosure agreements with clients/vendors  
• Company business plans |
Which do you prefer?

The generalized format for expressing the security category, SC, of an information system is:

\[ SC \text{ information system} = \{(\text{confidentiality, impact}), (\text{integrity, impact}), (\text{availability, impact})\}, \]

where the acceptable values for potential impact are LOW, MODERATE, or HIGH.

Why?
Data Retention

Why have a formal data retention policy?

a) Applicable Laws and Regulations
b) Resource Limits
c) Privacy
d) Access
e) Security
f) Plagiarism and Copyright
g) Enforcement
Data Retention

Why companies need to have a formal data retention policy...

• Practical Concerns
• Regulatory Concerns
• Privacy Concerns
Data Retention

Why companies need to have a formal data retention policy...

• Practical Concerns
Data Retention

Why companies need to have a formal data retention policy...

✓ Practical Concerns
• Regulatory Concerns

---

DIRECTIVE 2006/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 15 March 2006
on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 95 thereof,

Having regard to the proposal from the Commission,

Having regard to the Opinion of the European Economic and Social Committee (1),

Acting in accordance with the procedure laid down in Article 251 of the Treaty (2),

erased or made anonymous when no longer needed for the purpose of the transmission of a communication, except for the data necessary for billing or interconnection payments. Subject to consent, certain data may also be processed for marketing purposes and the provision of value-added services.

Article 15(1) of Directive 2002/58/EC sets out the conditions under which Member States may restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of that Directive. Any such restrictions must be necessary, appropriate and proportionate within a democratic society for specific public order purposes, i.e. to safeguard national security (i.e. State security), defence, public security or the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communications systems.
Data Retention

Why companies need to have a formal data retention policy...

✓ Practical Concerns
✓ Regulatory Concerns
• Privacy Concerns

www.dataretentionisnosolution.com

• Support Petition Against Data Retention
The EDRI and XS4ALL petition against data retention has attracted almost 42,000 signatures, of which over 16,000 are from the Netherlands (where the campaign was launched) and over 5,000 from Germany and Finland. Runners-up in the daily country count are Sweden and Bulgaria (almost 2,000 each), followed by Austria (almost 1,500) and Italy (well over 1,000). Belgium, Slovenia and France have each almost reached 1,000 signatures.

Currently, 66 organizations and companies have signed in support of the petition. The petition is now available in 17 languages.
Data Retention

Establishing a Data Retention Policy

- Establish data classes
- Classify data
- Establish retention periods
- Select archive methods
  - Paper-based
  - Electronic forms
Data Retention

Establishing a Data Retention Policy

✓ Establish data classes
✓ Classify data
✓ Establish retention periods
✓ Select archive methods
  • Paper-based
  • Electronic forms
• Create end-of-life processes
• Create policies for destruction of media
Data Retention

Establishing a Data Retention Policy

- Establish data classes
- Classify data
- Establish retention periods
- Select archive methods
  - Paper-based
  - Electronic forms
- Create end-of-life processes
- Create policies for destruction
- Identify roles and responsibilities
- Create enforcement mechanisms

<table>
<thead>
<tr>
<th>Owner</th>
<th>Steward</th>
<th>Custodian</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manages the business function that generates and/or uses the data</td>
<td>Focuses on managing data content and the business logic behind all data transformations.</td>
<td>Oversees the safe transport and storage of data</td>
</tr>
<tr>
<td>Has business and/or regulatory responsibility for data quality and management</td>
<td></td>
<td>Focuses on the underlying infrastructure and activities required to keep the data intact</td>
</tr>
</tbody>
</table>
Data Retention

Establishing a Data Retention Policy

- Establish data classes
- Classify data
- Establish retention periods
- Select archive methods
  - Paper-based
  - Electronic forms
- Create end-of-life processes
- Create policies for destruction of media
- Identify roles and responsibilities
- Create enforcement mechanisms
Data Retention

Handling Customer Data

- Conduct an enterprise application compliance review
- Implement Payment Application Data Security Standard (PA-DSS)

Requirements

For a payment application to be deemed PA-DSS compliant, software vendors must ensure that their software includes the following fourteen protections:[2]

1. Do not retain full magnetic stripe, card validation code or value, or PIN block data.
2. Protect stored cardholder data.
3. Provide secure authentication features.
4. Log payment application activity.
5. Develop secure payment applications.
6. Protect wireless transmissions.
7. Test payment applications to address vulnerabilities and maintain payment application updates.
8. Facilitate secure network implementation.
9. Cardholder data must never be stored on a server connected to The Internet.
10. Facilitate secure remote access to payment application.
11. Encrypt sensitive traffic over public networks.
12. Encrypt all non-console administrative access.
14. Assign PA-DSS responsibilities for personnel, and maintain training programs for personnel, customers, resellers, and integrators.
Data Retention

Handling Customer Data

- Conduct an enterprise application compliance review
- Implement Payment Application Data Security Standard (PA-DSS)
- Pilot data tokenization solutions
- Implement end-to-end encryption
- Restrict Internal access to customer data
Test Taking Tip

- Look for “subset” questions -

Often you will encounter questions that ask you to chose the “Best” answer...

The idea is: At least two of the answers are correct in some sense, but one is “more correct” than the others.

It can be useful to view these types of questions as having some possible answers that are actually subsets of the most correct answer.
Test Taking Tip

Example:

An attack that involves an attacker creates a misleading context in order to trick a user into making an inappropriate security-relevant decision is known as:

a) Spoofing attack  b) Surveillance attack  c) Social engineering attack  d) Man-in-the-middle attack

Answer: C
Test Taking Tip

Example:

An attack that involves an attacker creates a misleading context in order to trick a user into making an inappropriate security-relevant decision is known as:

a) Spoofing attack  b) Surveillance attack  c) Social engineering attack  d) Man-in-the-middle attack

Answer: C
Example:

An attack that involves an attacker creates a misleading context in order to trick a user into making an inappropriate security-relevant decision is known as:

a) Spoofing attack  b) Surveillance attack  c) Social engineering attack  d) Man-in-the-middle attack

Answer: C
Quiz