

Information security classification

v1.0

©2003 by [Lubomir Nistor](#)

Introduction

Information security or information protection is a big word right now and very often used to state how well treated the data is and how difficult it is to gain access to them via non-officially approved channels.

Now despite the fact that not all the information needs to be protected very often companies or even public sector doesn't distinguish public data from confidential data and protects them on the same level.

This document won't describe how to protect this information but more describe a way how to differentiate the protection for various types of information.

It surely is important to secure the customer data (as prescribed by law in many countries) but why to waste resource on protecting information about our already known products or newsletters.

Many banks with introduction of secure internet-banking moved their advisory products or newsletters under the password or PIN protected area making future customers desperate about the lack of information they need to decide whether to choose this or that bank.

On the other hand it is easy to gain access to vital information on some government or military sites allowing access to field manuals or system architecture description.

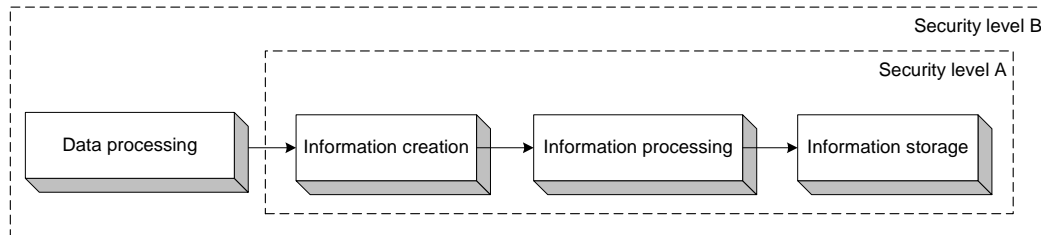
This shows the lack of understanding what information needs to be protected and how. Although there are many experts in the field who are able to design effective systems for information classification it very often shows lack of understanding of security management on top management layer.

This document should add more clarification to information classification and management to allow top-managers to understand the concept of it.

Information collection

In the beginning of the information lifecycle information is being created by either collection or processing. Security starts immediately at this point in order to guarantee minimal risk level from the start.

Very often information is created from lower level of security and classified into higher level (example: documentation of the uranium storage in nuclear power plant, classified as B, would be processed to create vulnerabilities assessment of the storage, which would be classified as A).



Of course there are also cases of declassifying information or lowering the security level (example: security level A would be nuclear silo manuals which would be processed to generate skills-set for manning the nuclear silo operation, classified as B)

Information can be created by:

Action	Example
Processing already existing data	Report on army readiness
Performing research (generating ideas)	Intercontinental missile defence system research
Reflecting status or writing down facts	Weapons status in the Ammunition depot

What are we protecting?

People

- Government personnel
- Contractors
- Military personnel

Activities/Operations

- Intelligence collection/analysis
- Sensitive movement of operations/personnel/property
- Conduct of sensitive training
- Communications/networking
- RDT&E and sensitive technology
- Production of sensitive technology
- Protection of nuclear/chemical/biological materials
- Protection of weapons, explosives, and equipment

Information

- Classified
- Sensitive Compartmented Information
- Top Secret
- Secret
- Confidential
- Unclassified
- System designs
- Intellectual property
- Patents
- System capabilities/vulnerabilities
- Sensitive methods
- Sensitive financial data

Facilities

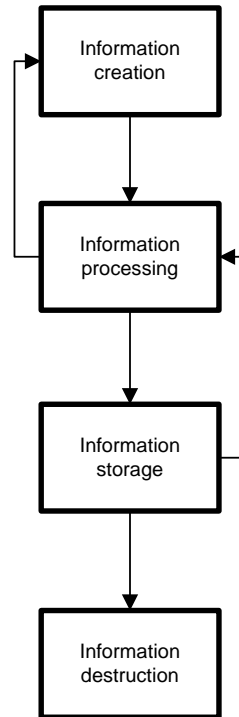
- Industry sites
- Headquarters
- Field offices/administrative buildings
- Training facilities
- Contractor facilities
- Storage facilities
- Production facilities
- R&D laboratories
- Power plants
- Parking facilities
- Aircraft hangars
- Residences

Equipment/Materials

- Transportation equipment/vehicles
- Maintenance equipment
- Operational equipment
- Communications equipment
- Security equipment
- Weapons
- Automated information systems equipment

Information lifecycle

In order to determine necessary protection for specific information it is necessary to understand how was this information created and how it would be used.



Information can be created either by having an idea or by processing already existing information.

Processing is done more in sense of updating and reviewing, but it is also forming the created information to fill into the shape or a standard.

After information is modified or created it is then stored, where it usually resides until it is needed again.

In case of unnecessary information the destruction is to take place, either to save storage space or to prevent information to be accessible to others in special cases.

There may be also other paths information can take, but they are not that common and are normally not considered in information classification.

Information classification

The process of classification is assessing the various attributes of information and putting them into classes and subclasses.

In order to start with classification process first step is to define attributes according to which information would be classified

Attributes

Attributes can vary from industry to industry but just to give an example from a defence industry:

- Type of weapons field (conventional, nuclear, chemical, biological, energetic,..)
- Freshness of information (new, only known to allies, known to industrial country armies, known to public)
- Research effort (1000 man-years, 100 man-years, 10 man-years, 1 man-year)
- Financial effort for production (100 mil Euro, 10 mil Euro, 1 mil Euro)
- Information value for others (100 mil Euro, 10 mil Euro, 1 mil Euro)

Class definition

After listing the attributes classes need to be defined and for each class there would be a list of attributes defined. It is important to put attributes together that do not exclude each other and can uniquely identify the class.

Here is an example of class definition from the previous list of attributes:

Class 1

Research effort: >1000 man-years
Financial effort for production: >100mil Euro
Information value to others: >100mil Euro

Class 2

Research effort: >1000 man-years
Financial effort for production: >100mil Euro
Information value to others: >100mil Euro

Class 3

Research effort: >10 man-years
Financial effort for production: >1mil Euro
Information value to others: >1mil Euro

Subclasses

Very often it is not easy to put attributes together that uniquely identify the subject, or enable proper security level for various types of information (nuclear information should be treated differently then conventional although the research effort is the same)

For subclass definition there may be a different attribute or set of attributes taken.

Subclass Nuclear:

Weapons type: Nuclear

Subclass Chemical

Weapons type: Chemical

Subclass Biological

Weapons type: Biological

Subclass Energetic

Weapons type: Energetic

Matrixes

Another possibility of class definition with many attributes would be defining an n-dimensional matrix with each dimension being one attribute (or one set of attributes).

Here is an example of the previous attributes in 2D matrix:

Attributes	100mil Euro value	10mil Euro value	1mil Euro value
Nuclear	Class 1	Class 2	Class 3
Biological	Class 4	Class 5	Class 6
Energetic	Class 7	Class 8	Class 9

Then for each class it is easier to define specific security level but it is hard to know all the attributes and specific class for the information, which would make classification process much difficult.

Information protection

Now we have information in classes and groups so we can assign specific protection methods to each one to ensure its security. There are many protection methods in the field of security and many of those are well known. Physical access controls are very often used and are effective as long as procedures are held by people involved.

Personnel clearance systems

In order to identify who has got access to information or not all systems are based on at least one of the following:

- Something you know (password)
- Something you have (ID badge)
- Something you are (biometrical variables like retina or fingerprint)

According to this information decisions are made whether to give access to the information or not.

Physical access controls

This category is very well known to many people as most of us are using it every day. From normal room with a key-lock up to a bunker far below surface with special magnetic lock blast doors guarded by a small defence force there can be no limits. The only limitation is the budget for protecting the information.

Computer access controls (or logical access controls)

Today there is most of the information stored on computers and its protection has to be ensured there as well. With established categories and classifications these systems should be flexible enough to enforce them. The following overview should display most commonly used methods.

Discretionary access control

Discretionary access control (DAC) is an access policy that restricts access to data based on the identity of users and/or the groups to which they belong.

There are 3 levels of identification hierarchy:

- Person (self)
- Group
- public

Rights to read write or execute are given specifically for each.

Although very common this system doesn't enforce the classifications very well unless data is properly distributed and classified. It lacks also flexibility to have exceptions or to give easily access to specific data somebody not from the group that this data actually belongs.

Mandatory access control

Systems providing mandatory access controls must assign sensitivity labels to *all* subjects (e.g., users, programs) and *all* objects (e.g., files, directories, devices, windows, sockets) in the system. A user's sensitivity label specifies the sensitivity level, or level of trust, associated with that user; it's often called a clearance. A file's

sensitivity label specifies the level of trust that a user must have to be able to access that file. Mandatory access controls use sensitivity labels to determine who can access what information in your system.

This means that user's rights are not specified per each data but according to the sensitivity labels.

MAC systems are used in high security areas protecting very sensitive information.

Role based access control

This access control system is based on assigning roles to the users by which they are permitted to gain access to information. A user can have many roles which allow him access to specific groups of data. Various functions are permitted to perform various actions (read/write/delete/execute/add/..) in order to process it.

This control system is used in modern operation systems which are used in security conscious environments.

Information handling procedures

Even if protective controls are in place they won't be very effective if people won't use them. Even if information is well protected while stored, it can be easily accessible while processing. Therefore procedures have to be in place to ensure that information is protected throughout the whole information life-cycle.

Information creation

- Classification
- marking

Information processing

- Declassification
- Anomaly/incident reporting
- dissemination

Information storage

- Backup
- Disaster recovery

Information destruction

- Safe destruction of information

Conclusion

Assessing the value or importance of information is vital part in security management and is one of the basic processes in risk assessment. In order for security policy to include also future enhancements or modifications to company or IT infrastructure there must be a guide to classify the new information in order to be able to deploy proper protective methods.

This document has shown the full lifecycle of information classification and should be of great help to security professionals to enhance their security policy with this part as well.

Leaders and managers should see now the importance of security classification and enhancements it brings into the company and its business risks minimisation. I hope they now also understand that security is not just buying some equipment with the word security in the description, but should be treated in more strategic way and be planned before the actual budget gets assigned to this.

Appendix 1. References

Security Classification of Information
Volume 2. Principles for Classification of Information
<http://www.fas.org/sgp/library/quist2/>

Security Classification of Information
Volume 1. Introduction, History, and Adverse Impacts
<http://www.fas.org/sgp/library/quist/>

Information classification from Security handbook
<http://www.boran.com/security/IT1x-4.html>

DSS way of teaching US people security (and classification in DoD)
<http://www.dss.mil/training/tsb.pdf>

Marking - DoD Guide to Marking Classified Documents
<http://www.dss.mil/isec/marking/index.htm>

NATO SECURITY PROCEDURES
http://www.fas.org/sgp/library/ipshbook/Chap_10.html

Classification of US DoC
<http://www.wasc.noaa.gov/wrso/securitymanual/>

GUIDE FOR MAPPING TYPES OF INFORMATION AND INFORMATION
SYSTEMS TO SECURITY CATEGORIES
<http://csrc.nist.gov/publications/nistpubs/800-60/SP800-60V1-final.pdf>

Appendix 2 Nondisclosure agreement form

SENSITIVE COMPARTMENTED INFORMATION NONDISCLOSURE STATEMENT	
<u>PRIVACY ACT STATEMENT</u>	
<u>AUTHORITY:</u>	EO 9397, November 1943 (SSN).
<u>PRINCIPAL PURPOSE(S):</u>	The information contained herein will be used to precisely identify individuals when it is necessary to certify their access to sensitive compartmented information.
<u>ROUTINE USE(S):</u>	Blanket routine uses, as published by Defense Intelligence Agency in the Federal Register.
<u>DISCLOSURE:</u>	Voluntary; however, failure to provide requested information may result in delaying the processing of your certification.
<u>SECTION A</u>	
An Agreement Between _____ and the United States. <small>(Printed or Typed Name)</small>	
<p>1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to information or material protected within Special Access Programs, hereinafter referred to in this Agreement as Sensitive Compartmented Information (SCI). I have been advised that SCI involves or derives from intelligence sources or methods and is classified or in the process of a classification determination under the standards of Executive Order 12356 or other Executive order or statute. I understand and accept that by being granted access to SCI, special confidence and trust shall be placed in me by the United States Government.</p> <p>2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of SCI, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and I understand these procedures. I understand that I may be required to sign subsequent agreements upon being granted access to different categories of SCI. I further understand that all my obligations under this Agreement continue to exist whether or not I am required to sign such subsequent agreements.</p> <p>3. I have been advised that unauthorized disclosure, unauthorized retention, or negligent handling of SCI by me could cause irreparable injury to the United States or be used to advantage by a foreign nation. I hereby agree that I will never divulge anything marked as SCI or that I know to be SCI to anyone who is not authorized to receive it without prior written authorization from the United States Government department or agency (hereinafter Department or Agency) that last authorized my access to SCI. I understand that it is my responsibility to consult with appropriate management authorities in the Department or Agency that last authorized my access to SCI, whether or not I am still employed by or associated with that Department or Agency or a contractor thereof, in order to ensure that I know whether information or material within my knowledge or control that I have reason to believe might be SCI, or related to or derived from SCI, is considered by such Department or Agency to be SCI. I further understand that I am also obligated by law and regulation not to disclose any classified information or material in an unauthorized fashion.</p> <p>4. In consideration of being granted access to SCI and of being assigned or retained in a position of special confidence and trust requiring access to SCI, I hereby agree to submit for security review by the Department or Agency that last authorized my access to such information or material, any writing or other preparation in any form, including a work of fiction, that contains or purports to contain any SCI or description of activities that produce or relate to SCI or that I</p>	<p>4. <i>(Continued)</i> have reason to believe are derived from SCI, that I contemplate disclosing to any person not authorized to have access to SCI or that I have prepared for public disclosure. I understand and agree that my obligation to submit such preparations for review applies during the course of my access to SCI and thereafter, and I agree to make any required submissions prior to discussing the preparation with, or showing it to, anyone who is not authorized to have access to SCI. I further agree that I will not disclose the contents of such preparation to any person not authorized to have access to SCI until I have received written authorization from the Department or Agency that last authorized my access to SCI that such disclosure is permitted.</p> <p>5. I understand that the purpose of the review described in paragraph 4 is to give the United States a reasonable opportunity to determine whether the preparation submitted pursuant to paragraph 4 set forth any SCI. I further understand that the Department or Agency to which I have made a submission will act upon them, coordinating within the Intelligence Community when appropriate, and make a response to me within a reasonable time, not to exceed 30 working days from date of receipt.</p> <p>6. I have been advised that any breach of this Agreement may result in the termination of my access to SCI and removal from a position of special confidence and trust requiring such access, as well as the termination of my employment or other relationships with any Department or Agency that provides me with access to SCI. In addition, I have been advised that any unauthorized disclosure of SCI by me may constitute violations of United States criminal laws, including the provisions of Sections 793, 794, 798, and 952, Title 18, United States Code, and of Section 783(b), Title 50, United States Code. Nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.</p> <p>7. I understand that the United States Government may seek any remedy available to it to enforce this Agreement, including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement. I have been advised that the action can be brought against me in any of the several appropriate United States District Courts where the United States Government may elect to file the action. Court costs and reasonable attorneys' fees incurred by the United States Government may be assessed against me if I lose such action.</p> <p>8. I understand that all information to which I may obtain access by signing this Agreement is now and will remain the property of the United States Government unless and until otherwise determined by an appropriate official or final ruling of a</p>

DD FORM 1847-1, DEC 91 (EG)

PREVIOUS EDITIONS ARE OBSOLETE.

Designed using Perform Pro, WHS/DIOR, Jun 94

<p>8. <i>(Continued)</i> court of law. Subject to such determination, I do not now, nor will I ever, possess any right, interest, title or claim whatsoever to such information. I agree that I shall return all materials that may have come into my possession or for which I am responsible because of such access, upon demand by an authorized representative of the United States Government or upon the conclusion of my employment or other relationship with the United States Government entity providing me access to such materials. If I do not return such materials upon request, I understand this may be a violation of Section 793, Title 18, United States Code.</p> <p>9. Unless and until I am released in writing by an authorized representative of the Department or Agency that last provided me with access to SCI, I understand that all the conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to SCI, and at all times thereafter.</p> <p>10. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect. This Agreement concerns SCI and does not set forth such other conditions and obligations not related to SCI as may now or hereafter pertain to my employment by or assignment or relationship with the Department or Agency.</p> <p>11. These restrictions are consistent with and do not supersede conflict with or otherwise alter the employee obligations, rights, or liabilities created by Executive Order 12356; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act</p>	<p>11. <i>(Continued)</i> (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 USC 421 et seq.) (governing disclosures that could expose confidential Government agents), and the statutes which protect against disclosure that may compromise the national security, including Section 641, 793, 794, 798, and 952 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 USC Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this agreement and are controlling.</p> <p>12. I have read this Agreement carefully and my questions, if any, have been answered to my satisfaction. I acknowledge that the briefing officer has made available Sections 793, 794, 798, and 952 of Title 18, United States Code, and Section 783(b) of Title 50, United States Code, and Executive Order 12356, as amended, so that I may read them at this time, if I so choose.</p> <p>13. I hereby assign to the United States Government all rights, title and interest, and all royalties, remunerations, and emoluments that have resulted, will result, or may result from any disclosure, publication, or revelation not consistent with the terms of this Agreement.</p> <p>14. This Agreement shall be interpreted under and in conformance with the laws of the United States.</p> <p>15. I make this Agreement without any mental reservation or purpose of evasion.</p>		
16. TYPED OR PRINTED NAME <i>(Last, First, Middle Initial)</i>	17. GRADE/RANK/SVC	18. SOCIAL SECURITY NO.	19. BILLET NO. <i>(Optional)</i>
20. ORGANIZATION	21. SIGNATURE		22. DATE SIGNED <i>(YYMMDD)</i>
FOR USE BY MILITARY AND GOVERNMENT CIVILIAN PERSONNEL			
SECTION B			
The execution of this Agreement was witnessed by the undersigned, who accepted it on behalf of the United States Government as a prior condition of access to Sensitive Compartmented Information.			
23. TYPED OR PRINTED NAME <i>(Last, First, Middle Initial)</i>	24. ORGANIZATION		
25. SIGNATURE			26. DATE SIGNED <i>(YYMMDD)</i>
FOR USE BY CONTRACTORS/CONSULTANTS/NON-GOVERNMENT PERSONNEL			
SECTION C			
The execution of this Agreement was witnessed by the undersigned.			
27. TYPED OR PRINTED NAME <i>(Last, First, Middle Initial)</i>	28. ORGANIZATION		
29. SIGNATURE			30. DATE SIGNED <i>(YYMMDD)</i>
SECTION D			
This Agreement was accepted by the undersigned on behalf of the United States Government as a prior condition of access to Sensitive Compartmented Information.			
31. TYPED OR PRINTED NAME <i>(Last, First, Middle Initial)</i>	32. ORGANIZATION		
33. SIGNATURE			34. DATE SIGNED <i>(YYMMDD)</i>

DD FORM 1847-1, DEC 91 (BACK)

Reset