

Classified information

Classified information is material that a government body deems to be sensitive information that must be protected. Access is restricted by law or regulation to particular groups of people with the necessary security clearance and need to know, and mishandling of the material can incur criminal penalties.

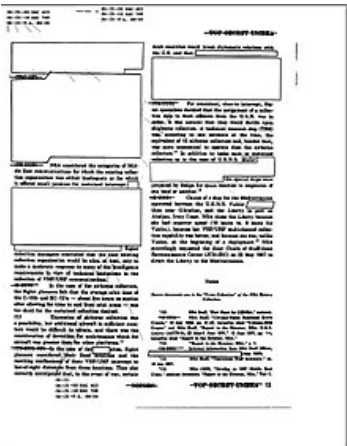
A formal security clearance is required to view or handle classified documents or to access classified data. The clearance process requires a satisfactory background investigation. Documents and other information must be properly marked "by the author" with one of several (hierarchical) levels of sensitivity—e.g. restricted, confidential, secret, and top secret. The choice of level is based on an impact assessment; governments have their own criteria, including how to determine the classification of an information asset and rules on how to protect information classified at each level. This process often includes security clearances for personnel handling the information.

Although "classified information" refers to the formal categorization and marking of material by level of sensitivity, it has also developed a sense synonymous with "censored" in US English. A distinction is often made between formal security classification and privacy markings such as "commercial in confidence". Classifications can be used with additional keywords that give more detailed instructions on how data should be used or protected.

Some corporations and non-government organizations also assign levels of protection to their private information, either from a desire to protect trade secrets, or because of laws and regulations governing various matters such as personal privacy, sealed legal proceedings and the timing of financial information releases.

With the passage of time much classified information can become a bit less sensitive, or becomes much less sensitive, and may be declassified and made public. Since the late twentieth century there has been freedom of information legislation in some countries, whereby the public is deemed to have the right to all information that is not considered to be damaging if released. Sometimes documents are released with information still considered confidential obscured (redacted), as in the adjacent example.

The question exists among some political science and legal experts, whether the definition of classified ought to be information that would cause injury to the cause of justice, human rights, etc., rather than information that would cause injury to the national interest, to distinguish when classifying information is in the collective best interest of a just society or merely the best interest of a society acting unjustly, to protect its people, government, or administrative officials from legitimate recourses consistent with a fair and just social contract.



A typical classified document. Page 13 of a U.S. National Security Agency report^[1] on the USS *Liberty* incident, partially declassified and released to the public in July 2004. The original overall classification of the page, "top secret", and the Special Intelligence code word "umbra", are shown at top and bottom. The classification of individual paragraphs and reference titles is shown in parentheses—there are six different levels on this page alone. Notations with leader lines at top and bottom cite statutory authority for not declassifying certain sections.

Contents
Government classification
Typical classification levels
<u>Top Secret (TS)</u>
<u>Secret</u>
<u>Confidential</u>
<u>Restricted</u>
<u>Official</u>
<u>Unclassified</u>
<u>Clearance</u>
<u>Compartmented information</u>
International
<u>NATO classifications</u>
<u>International organisations</u>
By country
<u>Australia</u>
<u>Brazil</u>
<u>Canada</u>
<u>Background and hierarchy</u>

Special operational information

Classified information

Protected information

People's Republic of China

France

Hong Kong

New Zealand

Romania

Russia

Sweden

Switzerland

Turkey

United Kingdom

United States

Table of equivalent classification markings in various countries

Corporate classification

Traffic Light Protocol

See also

References

External links

Government classification

The purpose of classification is to protect information. Higher classifications protect information that might endanger national security. Classification formalises what constitutes a "state secret" and accords different levels of protection based on the expected damage the information might cause in the wrong hands.

However, classified information is frequently "leaked" to reporters by officials for political purposes. Several U.S. presidents have leaked sensitive information to get their point across to the public.^{[2][3]}

Typical classification levels

Although the classification systems vary from country to country, most have levels corresponding to the following British definitions (from the highest level to lowest).

Top Secret (TS)

Top Secret is the highest level of classified information.^[4] Information is further compartmented so that specific access using a code word after *top secret* is a legal way to hide collective and important information.^[5] Such material would cause "exceptionally grave damage" to national security if made publicly available.^[6] Prior to 1942, the United Kingdom and other members of the British Empire used *Most Secret*, but this was later changed to match the United States' category name of *Top Secret* in order to simplify Allied interoperability.

The Washington Post reported in an investigation entitled *Top Secret America* that, as of 2010, "An estimated 854,000 people ... hold top-secret security clearances" in the United States.^[7]

Secret

Secret material would cause "serious damage" to national security if it were publicly available.^[10]

In the United States, operational "Secret" information can be marked with an additional "LIMDIS", to limit distribution.

Confidential

Confidential material would cause "damage" or be prejudicial to national security if publicly available.^[11]



KGB's "*List of traitors to the Motherland, agents of foreign intelligence, and other wanted state criminals*" (1979) seen in Museum of Genocide Victims, Vilnius: originally marked *top secret*

Restricted

Restricted material would cause "undesirable effects" if publicly available. Some countries do not have such a classification in public sectors, such as commercial industries. Such a level is also known as "*Private Information*".

Official

Official (Equivalent to US DOD classification FOUO – For Official Use Only) material forms the generality of government business, public service delivery and commercial activity. This includes a diverse range of information, of varying sensitivities, and with differing consequences resulting from compromise or loss. OFFICIAL information must be secured against a threat model that is broadly similar to that faced by a large private company.

The OFFICIAL SENSITIVE classification replaced the Restricted classification in April 2014 in the UK; OFFICIAL indicates the previously used UNCLASSIFIED marking.^[12]

Unclassified

Unclassified is technically not a classification level, but this is a feature of some classification schemes, used for government documents that do not merit a particular classification or which have been declassified. This is because the information is low-impact, and therefore does not require any special protection, such as vetting of personnel.

A plethora of pseudo-classifications exist under this category.

Clearance

Clearance is a general classification, that comprises a variety of rules controlling the level of permission required to view some classified information, and how it must be stored, transmitted, and destroyed. Additionally, access is restricted on a "need to know" basis. Simply possessing a clearance does not automatically authorize the individual to view all material classified at that level or below that level. The individual must present a legitimate "need to know" in addition to the proper level of clearance.

Compartmented information

In addition to the general risk-based classification levels, additional compartmented constraints on access exist, such as (in the U.S.) Special Intelligence (SI), which protects intelligence sources and methods, No Foreign dissemination (NOFORN), which restricts dissemination to U.S. nationals, and Originator Controlled dissemination (ORCON), which ensures that the originator can track possessors of the information. Information in these compartments is usually marked with specific keywords in addition to the classification level.

Government information about nuclear weapons often has an additional marking to show it contains such information (CNWDI).

International

When a government agency or group shares information between an agency or group of other country's government they will generally employ a special classification scheme that both parties have previously agreed to honour.

For example, the marking ATOMAL, is applied to U.S. RESTRICTED DATA or FORMERLY RESTRICTED DATA and United Kingdom ATOMIC information that has been released to NATO. ATOMAL information is marked COSMIC TOP SECRET ATOMAL (CTSA), NATO SECRET ATOMAL (NSAT), or NATO CONFIDENTIAL ATOMAL (NCA).

NATO classifications

For example, sensitive information shared amongst NATO allies has four levels of security classification; from most to least classified:^{[13][14]}

1. COSMIC TOP SECRET (CTS)
2. NATO SECRET (NS)
3. NATO CONFIDENTIAL (NC)
4. NATO RESTRICTED (NR)

A special case exists with regard to NATO UNCLASSIFIED (NU) information. Documents with this marking are NATO property (copyright) and must not be made public without NATO permission.

"It is desired that no document be released which refers to experiments with humans and might have adverse effect on public opinion or result in legal suits. Documents covering such work field should be classified 'secret'."

April 17, 1947 Atomic Energy Commission memo from Colonel O.G. Haywood, Jr. to Dr. Fidler at the Oak Ridge Laboratory in Tennessee.^[8] As of 2010, Executive Order 13526 bans classification of documents simply to "conceal violations of law, inefficiency, or administrative error" or "prevent embarrassment to a person, organization, or agency".^[9]

COSMIC is an abbreviation for "Control Of Secret Material in an International Command",^[15]

International organisations

- The European Union has four levels: EU TOP SECRET, EU SECRET, EU CONFIDENTIAL, EU RESTRICTED.^[16] (Note that usually the French terms are used.)
 - **TRÈS SECRET UE/EU TOP SECRET**: information and material the unauthorised disclosure of which could cause exceptionally grave prejudice to the essential interests of the European Union or of one or more of the Member States;
 - **SECRET UE/EU SECRET**: information and material the unauthorised disclosure of which could seriously harm the essential interests of the European Union or of one or more of the Member States;
 - **CONFIDENTIEL UE/EU CONFIDENTIAL**: information and material the unauthorised disclosure of which could harm the essential interests of the European Union or of one or more of the Member States;
 - **RESTREINT UE/EU RESTRICTED**: information and material the unauthorised disclosure of which could be disadvantageous to the interests of the European Union or of one or more of the Member States.
- Organisation for Joint Armament Cooperation, a European defence organisation, has three levels of classification: OCCAR SECRET, OCCAR CONFIDENTIAL, and OCCAR RESTRICTED.^[17]
- ECIPS, the European Centre for Information Policy and Security, has 4 levels of Security Information, COSMIC (TOP SECRET), EC-SECRET, EC-CONFIDENTIAL and EC-COMMITTEES.^[18]

By country

Most countries employ some sort of classification system for certain government information. For example, in Canada, information that the U.S. would classify SBU (Sensitive but Unclassified) is called "protected" and further subcategorised into levels A, B, and C.

Australia

On 19 July 2011, the National Security (NS) classification marking scheme and the Non-National Security (NNS) classification marking scheme in Australia was unified into one structure.

The Australian Government Security Classification system now comprises TOP SECRET, SECRET, CONFIDENTIAL and PROTECTED. A new dissemination limiting markers (DLMs) scheme was also introduced for information where disclosure may be limited or prohibited by legislation, or where it may otherwise require special handling. The DLM marking scheme comprises For Official Use Only (FOUO), Sensitive, Sensitive: Personal, Sensitive: Legal, and Sensitive: Cabinet.^[19]

Documents marked Sensitive Cabinet, relating to discussions in Federal Cabinet, are treated as PROTECTED at minimum due to its higher sensitivity.

Brazil

There are three levels of document classification under Brazilian Information Access Law (http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/Lei/L12527.htm): *ultrassecreto* (top secret), *secreto* (secret) and *reservado* (restricted).

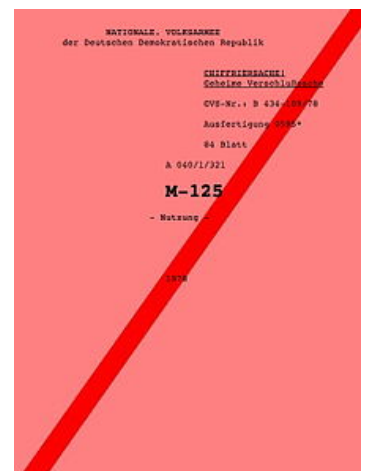
A top secret (*ultrassecreto*) government-issued document may be classified for a period of 25 years, which may be extended up to another 25 years. Thus, no document remains classified for more than 50 years. This is mandated by the 2011 Information Access Law (*Lei de Acesso à Informação*), a change from the previous rule, under which documents could have their classification time length renewed indefinitely, effectively shuttering state secrets from the public. The 2011 law applies retroactively to existing documents.

Canada

Background and hierarchy

The Government of Canada employs two main types of sensitive information designation: *Classified* and *Protected*. The access and protection of both types of information is governed by the Security of Information Act, effective December 24, 2001, replacing the *Official Secrets Act 1981*.^[20] To access the information, a person must have the appropriate security clearance and the need to know.

In addition, the caveat "Canadian Eyes Only" is used to restrict access to Classified or Protected information only to Canadian citizens with the appropriate security clearance and need to know.^[21]



Facsimile of the cover page from an East German operation manual for the M-125 Fialka cipher machine. The underlined classification markings can be translated as "Cryptologic material! Secret restricted material" de:Verschlusssache.

Special operational information

SOI is not a classification of data *per se*. It is defined under the *Security of Information Act*, and unauthorised release of such information constitutes a higher breach of trust, with penalty of life imprisonment.

SOIs include:

- military operations in respect of a potential, imminent or present armed conflict
- the identity of confidential source of information, intelligence or assistance to the Government of Canada
- tools used for information gathering or intelligence
- the object of a covert investigation, or a covert collection of information or intelligence
- the identity of any person who is under covert surveillance
- encryption and cryptographic systems
- information or intelligence to, or received from, a foreign entity or terrorist group

Classified information

Classified information can be designated *Top Secret*, *Secret* or *Confidential*. These classifications are only used on matters of national interest.

- Top Secret: applies when compromise might reasonably cause exceptionally grave injury to the national interest. The possible impact must be great, immediate and irreparable.
- Secret: applies when compromise might reasonably cause serious injury to the national interest.
- Confidential: disclosure might reasonably cause injury to the national interest.

Protected information

Protected information is not classified. It pertains to any sensitive information that does not relate to national security and cannot be disclosed under the access and privacy legislation because of the potential injury to particular public or private interests.^{[22][23]}

- Protected C (Extremely Sensitive protected information): designates extremely sensitive information, which if compromised, could reasonably be expected to cause extremely grave injury outside the national interest. Examples include bankruptcy, identities of informants in criminal investigations, etc.
- Protected B (Particularly Sensitive protected information): designates information that could cause severe injury or damage to the people or group involved if it was released. Examples include medical records, annual personnel performance reviews, income tax returns, etc.
- Protected A (Low-Sensitive protected information): designates low sensitivity information that should not be disclosed to the public without authorization and could reasonably be expected to cause injury or embarrassment outside the national interest. Example of Protected A information include employee identification number, pay deposit banking information, etc.

Federal Cabinet (Queen's Privy Council for Canada) papers are either protected (e.g., overhead slides prepared to make presentations to Cabinet) or classified (e.g., draft legislation, certain memos).^[24]

People's Republic of China

The Criminal Law of the People's Republic of China (which is not operative in the Special Administrative Regions of Hong Kong and Macau) makes it a crime to release a state secret. Regulation and enforcement is carried out by the National Administration for the Protection of State Secrets.

Under the 1989 "Law on Guarding State Secrets,"^[25] state secrets are defined as those that concern:

1. Major policy decisions on state affairs
2. The building of national defence and in the activities of the armed forces
3. Diplomatic activities and in activities related to foreign countries and those to be maintained as commitments to foreign countries
4. National economic and social development
5. Science and technology
6. Activities for preserving state security and the investigation of criminal offences
7. Any other matters classified as "state secrets" by the national State Secrets Bureau^[26]

Secrets can be classified into three categories:



A building in Wuhan housing provincial offices for dealing with foreign countries etc. The red slogan says, "Protection of national secrets is a duty of every citizen".

- Top secret (绝密): defined as "vital state secrets whose disclosure would cause extremely serious harm to state security and national interests"
- Highly secret (机密): defined as "important state secrets whose disclosure would cause serious harm to state security and national interests"
- Secret (秘密): defined as "ordinary state secrets whose disclosure would cause harm to state security and national interests"^[26]

France

In France, classified information is defined by article 413-9 of the Penal Code.^[27] The three levels of military classification are

- *Très Secret Défense* (Very Secret Defence): Information deemed extremely harmful to national defense, and relative to governmental priorities in national defense. No service or organisation can elaborate, process, stock, transfer, display or destroy information or protected supports classified at this level without authorization from the Prime Minister or the national secretary for National Defence. Partial or exhaustive reproduction is strictly forbidden.
- *Secret Défense* (Secret Defence): Information deemed very harmful to national defense. Such information cannot be reproduced without authorisation from the emitting authority, except in exceptional emergencies.
- *Confidentiel Défense* (Confidential Defence): Information deemed potentially harmful to national defense, or that could lead to uncovering some information classified at a higher level of security.

Less sensitive information is "protected". The levels are

- *Confidentiel personnels Officiers* ("Confidential officers")
- *Confidentiel personnels Sous-Officiers* ("Confidential non-commissioned officers")
- *Diffusion restreinte* ("restricted information")
- *Diffusion restreinte administrateur* ("administrative restricted information")
- *Non Protégé* (unprotected)

A further caveat, "*spécial France*" (reserved France) restricts the document to French citizens (in its entirety or by extracts). This is not a classification level.

Declassification of documents can be done by the *Commission consultative du secret de la défense nationale* (CCSDN), an independent authority. Transfer of classified information is done with double envelopes, the outer layer being plastified and numbered, and the inner in strong paper. Reception of the document involves examination of the physical integrity of the container and registration of the document. In foreign countries, the document must be transferred through specialised military mail or diplomatic bag. Transport is done by an authorised convoyer or habilitated person for mail under 20 kg. The letter must bear a seal mentioning "*PAR VALISE ACCOMPAGNEE-SACOCHE*". Once a year, ministers have an inventory of classified information and supports by competent authorities.

Once their usage period is expired, documents are transferred to archives, where they are either destroyed (by incineration, crushing, or overvoltage), or stored.

In case of unauthorized release of classified information, competent authorities are the Ministry of Interior, the *Haut fonctionnaire de défense et de sécurité* ("high civil servant for defence and security") of the relevant ministry, and the General secretary for National Defence. Violation of such secrets is an offence punishable with 7 years of imprisonment and a 100,000 Euro fine; if the offence is committed by imprudence or negligence, the penalties are 3 years of imprisonment and a 45,000 Euro fine.

Hong Kong

The Security Bureau is responsible for developing policies in regards to the protection and handling of confidential government information. In general, the system used in Hong Kong is very similar to the UK system, developed from the Colonial Hong Kong era.

Four classifications exists in Hong Kong, from highest to lowest in sensitivity:^[28]

- Top Secret (絕對機密)
- Secret (高度機密)
- Confidential (機密)
 - Temporary Confidential (臨時保密)
- Restricted (限閱文件/內部文件)
 - Restricted (staff) (限閱文件(人事))
 - Restricted (tender) (限閱文件 (投標))

Turkey

According to the related regulations in [Turkey](#), there are four levels of document classification:^[34] *çok gizli* (top secret), *gizli* (secret), *özel* (confidential) and *hizmete özel* (restricted). The fifth "inscription" is *tasnif dışı*, which means unclassified.

United Kingdom

Until 2013, the [United Kingdom](#) used five levels of classification—from lowest to highest, they were: PROTECT, RESTRICTED, CONFIDENTIAL, SECRET and TOP SECRET (formerly MOST SECRET). The [Cabinet Office](#) provides guidance on how to protect information, including the security clearances required for personnel. Staff may be required to sign to confirm their understanding and acceptance of the Official Secrets Acts 1911 to 1989, although the Act applies regardless of signature. PROTECT is not in itself a security protective marking level (such as RESTRICTED or greater), but is used to indicate information which should not be disclosed because, for instance, the document contains tax, national insurance, or other personal information.

Government documents without a classification may be marked as UNCLASSIFIED or NOT PROTECTIVELY MARKED.^[35]

This system was replaced by the [Government Security Classifications Policy](#), which has a simpler model: TOP SECRET, SECRET, and OFFICIAL from April 2014.^[12] OFFICIAL SENSITIVE is a security marking which may be followed by one of three authorised descriptors: COMMERCIAL, LOCSEN (location sensitive) or PERSONAL. SECRET and TOP SECRET may include a caveat such as UK EYES ONLY.

Also useful is that scientific discoveries may be classified via the [D-Notice](#) system if they are deemed to have applications relevant to national security. These may later emerge when technology improves so for example the specialised processors and routing engines used in graphics cards are loosely based on top secret military chips designed for code breaking and image processing. They may or may not have safeguards built in to generate errors when specific tasks are attempted and this is invariably independent of the card's operating system.

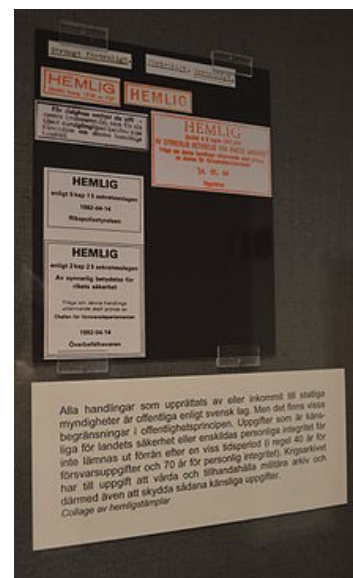
United States

The U.S. classification system is currently established under [Executive Order 13526](#) and has three levels of classification—Confidential, Secret, and Top Secret. The U.S. had a Restricted level during [World War II](#) but no longer does. U.S. regulations state that information received from other countries at the Restricted level should be handled as Confidential. A variety of markings are used for material that is not classified, but whose distribution is limited administratively or by other laws, e.g., For Official Use Only (FOUO), or Sensitive but Unclassified (SBU). The Atomic Energy Act of 1954 provides for the protection of information related to the design of nuclear weapons. The term "Restricted Data" is used to denote certain nuclear technology. Information about the storage, use or handling of nuclear material or weapons is marked "Formerly Restricted Data". These designations are used in addition to level markings (Confidential, Secret and Top Secret). Information protected by the Atomic Energy Act is protected by law and information classified under the Executive Order is protected by Executive privilege.

The U.S. government insists it is "not appropriate" for a court to question whether any document is legally classified.^[36] In the 1973 trial of [Daniel Ellsberg for releasing the Pentagon Papers](#), the judge did not allow any testimony from Ellsberg, claiming it was "irrelevant", because the assigned classification could not be challenged. The charges against Ellsberg were ultimately dismissed after it was revealed that the government had broken the law in secretly breaking into the office of Ellsberg's psychiatrist and in tapping his telephone without a warrant. Ellsberg insists that the legal situation in the U.S. today is worse than it was in 1973, and [Edward Snowden](#) could not get a fair trial.^[37] The [State Secrets Protection Act](#) of 2008 might have given judges the authority to review such questions *in camera*, but the bill was not passed.^[36]

When a government agency acquires classified information through covert means, or designates a program as classified, the agency asserts "ownership" of that information and considers any public availability of it to be a violation of their ownership — even if the same information was acquired independently through "parallel reporting" by the press or others. For example, although the [CIA drone program](#) has been widely discussed in public since the early 2000s, and reporters personally observed and reported on drone missile strikes, the CIA still considers the very existence of the program to be classified in its entirety, and any public discussion of it technically constitutes exposure of classified information. "Parallel reporting" was an issue in determining what constitutes "classified" information during the [Hillary Clinton email controversy](#) when Assistant Secretary of State for Legislative Affairs Julia Frifield noted, "When policy officials obtain information from open sources, 'think tanks,' experts, foreign government officials, or others, the fact that some of the information may also have been available through intelligence channels does not mean that the information is necessarily classified."^{[38][39][40]}

Table of equivalent classification markings in various countries



Some Swedish examples of markings attached to documents that are to be kept secret. A single frame around the text indicates *Hemlig*, which can be equal to either Secret, Confidential or Restricted. Double frames means *Kvalificerat hemlig*, that is, Top Secret.



Security classifications in the UK

(State)	Top Secret	Secret	Confidential	Restricted
<u>Albania</u>	Teper Sekret	Sekret	Konfidencial	I Kufizuar
<u>Argentina</u>	Estrictamente Secreto y Confidencial	Secreto	Confidencial	Reservado
<u>Australia</u>	Top Secret	Secret	Confidential	Protected
<u>Austria</u>	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
<u>Belgium</u>	Zeer Geheim / Très Secret	Geheim / Secret	Vertrouwelijk / Confidentiel	Beperkte Verspreiding / Diffusion restreinte
<u>Bolivia</u>	Supersecreto or Muy Secreto	Secreto	Confidencial	Reservado
<u>Bosnia and Herzegovina</u>	Vrlo tajno	Tajno	Povjerljivo	Interno
<u>Brazil</u>	Ultrassecreto	Secreto	no equivalent (formerly <i>Confidencial</i>)	Reservado
<u>Bulgaria</u>	<i>Strògo sècretno</i> Строго секретно	<i>Sècretno</i> Секретно	<i>Poveritèlno</i> Поверително	<i>Za služebno polzvàne</i> За служебно ползване
<u>Cambodia</u>	Sam Ngat Bamphot	Sam Ngat Roeung	Art Kambang	Ham Kom Psay
<u>Canada</u>	Top Secret/Très secret	Secret/Secret	Confidential/Confidentiel	Protected A, B or C / Protégé A, B ou C
<u>Chile</u>	Secreto	Secreto	Reservado	Reservado
<u>China</u>	Juémì (绝密)	Jīmì (机密)	Mìmì (秘密)	Nèibù (内部)
<u>Colombia</u>	Ultrassecreto	Secreto	Confidencial	Reserva del sumario
<u>Costa Rica</u>	Alto Secreto	Secreto	Confidencial	
<u>Croatia</u>	Vrlo tajno	Tajno	Povjerljivo	Ograničeno
<u>Czech Republic</u>	Přísně tajné	Tajné	Důvěrné	Vyhrazené
<u>Denmark</u>	Yderst Hemmeligt (YHM)	Hemmeligt (HEM)	Fortroligt (FTR)	Til Tjenestebrug (TTJ) Foreign Service: Fortroligt (thin Black border)
<u>Ecuador</u>	Secretísimo	Secreto	Confidencial	Reservado
<u>Egypt</u>	<i>Sirriy lil-Gāyah</i> سري للغاية	<i>Sirriy Ġiddan</i> سري جداً	<i>Khāṣ</i> خاص	<i>Maḥzūr</i> محظور
<u>El Salvador</u>	Ultra Secreto	Secreto	Confidencial	Reservado
<u>Estonia</u>	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
<u>Ethiopia</u>	ብርቱ ምስጢር	ምስጢር	ጥብቅ	ክልክል
<u>European Union (EU)</u>	TRES SECRET UE / EU TOP SECRET	SECRET UE / EU SECRET	CONFIDENTIEL UE / EU CONFIDENTIAL	RESTREINT UE / EU RESTRICTED
<u>European Union (Western) (WEU)</u>	FOCAL TOP SECRET	WEU SECRET	WEU CONFIDENTIAL	WEU RESTRICTED
<u>Euratom</u>	EURA TOP SECRET	EURA SECRET	EURA CONFIDENTIAL	EURA RESTRICTED
<u>Finland</u> ^[a]	Erittäin salainen (ST I)	Salainen (ST II)	Luottamuksellinen (ST III)	Käyttö rajoitettu (ST IV)
<u>France</u>	Très secret défense	Secret défense	Confidentiel défense	Diffusion restreinte
<u>Germany</u>	STRENG GEHEIM	GEHEIM	VS-VERTRAULICH	VS-NUR FÜR DEN DIENSTGEBRAUCH
<u>Greece</u>	Ἀκρῶς Απόρρητον	Απόρρητον	Εμπιστευτικόν	Περιορισμένης Χρήσης
<u>Guatemala</u>	Alto Secreto	Secreto	Confidencial	Reservado
<u>Haiti</u>	Top Secret	Secret	Confidential	Reserve
<u>Honduras</u>	Super Secreto	Secreto	Confidencial	Reservado
<u>Hong Kong</u>	Top Secret, 高度機密	Secret, 機密	Confidential, 保密	Restricted, 內部文件/限閱 文件
<u>Hungary</u>	Szigorúan Titkos	Titkos	Bizalmas	Korlátozott Terjesztésű

<u>India (Hindi)</u>	परम गुप्त (Param Gupt)	गुप्त (Gupt)	गोपनीय (Gopniya)	प्रतिबंधित/सीमित (Pratibandhit/seemit)
<u>India (English)</u>	Top Secret	Secret	Confidential	Restricted
<u>Indonesia</u>	Sangat Rahasia	Rahasia	Rahasia Dinas	Terbatas
<u>Iran</u>	Bekoli-Serri بکلی سری	Serri سری	Kheili-Mahramaneh خیلی محرمانه	Mahramaneh محرمانه
<u>Iraq</u>	Sirriy lil-Gāyah سري للغاية	Sirriy سري	Khāṣṣ خاص	Maḥdūd محدود
<u>Iceland</u>	Algert Leyndarmál	Leyndarmál	Trúnaðarmál	Þjónustuskjal
<u>Ireland (Irish language)</u>	An-sicreideach	Sicreideach	Runda	Srianta
<u>Israel</u>	Sodi Beyoter סודי ביותר	Sodi סודי	Shamur שמור	Mugbal מוגבל
<u>Italy</u>	Segretissimo	Segreto	Riservatissimo	Riservato
<u>Japan</u>	Kimitsu (機密)	Gokuhi (極秘)	Hi (秘)	Toriatsukaichuui (取り扱い注意)
<u>Jordan</u>	Maktūm Ġiddan مكتوم جداً	Maktūm مكتوم	Sirriy سري	Maḥdūd محدود
<u>South Korea</u>	1(II)-geup Bimil, 1급 비밀, 一級秘密	2(I)-geup Bimil, 2급 비밀, 二級秘密	3(Sam)-geup Bimil, 3급 비밀, 三級秘密	Daeoebi, 대외비, 對外秘
<u>Laos</u>	Lup Sood Gnod	Kuam Lup	Kuam Lap	Chum Kut Kon Arn
<u>Latvia</u>	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
<u>Lebanon</u>	Tres Secret	Secret	Confidentiel	
<u>Lithuania</u>	Visiškai Slaptai	Slaptai	Konfidencialiai	Riboto Naudojimo
<u>Malaysia</u>	Rahsia Besar	Rahsia	Sulit	Terhad
<u>Mexico</u>	Ultra Secreto	Secreto	Confidencial	Restringido
<u>Montenegro</u>	Strogo Tajno	Tajno	Povjerljivo	Interno
<u>Netherlands</u> ^[41]	STG. Zeer Geheim	STG. Geheim	STG. Confidentieel	Departementaal Vertrouwelijk
<u>New Zealand</u>	Top Secret	Secret	Confidential	Restricted
<u>Nicaragua</u>	Alto Secreto	Secreto	Confidencial	Reservado
<u>Norway</u>	STRENGT HEMMELIG	HEMMELIG	KONFIDENSIELT	BEGRENSET
<u>Pakistan (Urdu)</u>	Intahai Khufia انتہائی خفیہ	Khufia خفیہ	Sigh-e-Raz صیخہ راز	Baraj Mahdud Taqsim محدود تقسیم
<u>Pakistan (English)</u>	Top Secret	Secret	Confidential	Restricted
<u>Paraguay</u>	Secreto	Secreto	Confidencial	Reservado
<u>Peru</u>	Estrictamente Secreto	Secreto	Confidencial	Reservado
<u>Philippines (English)</u>	Top Secret	Secret	Confidential	Restricted
<u>Philippines (Tagalog)</u>	Matinding Lihim	Mahigpit na Lihim	Lihim	Ipinagbabawal
<u>Poland</u>	Ścisłe tajne	Tajne	Poufne	Zastrzeżone
<u>Portugal</u>	Muito Secreto	Secreto	Confidencial	Reservado
<u>Romania</u>	Strict Secret de Importanță Deosebită	Strict Secret	Secret	Secret de serviciu
<u>Russia</u>	Особой важности (вариант: Совершенно Секретно (Sovershenno Sekretno))	Совершенно секретно (вариант: Секретно (Sekretno))	Секретно (вариант: Не подлежит оглашению (Конфиденциально) (Ne podlezhit oglasheniyu (Konfidentsial'no))	Для Служебного Пользования (ДСП) (Dlya Sluzhebnogo Pol'zovaniya)
<u>Saudi Arabia</u>	Saudi Top Secret	Saudi Very Secret	Saudi Secret	Saudi Restricted
<u>Serbia</u>	Latin: Državna tajna Cyrillic: Државна тајна	Latin: Strogo poverljivo Cyrillic: Строго поверљиво	Latin: Poverljivo Cyrillic: Поверљиво	Latin: Interno Cyrillic: Интерно
<u>Singapore</u>	Top Secret	Secret	Confidential	Restricted
<u>Somalia</u>	Sir Muhiim ah	Sir Gooniya	Xog Qarsoon	Qarsoon

<u>Slovak Republic</u>	Prísne tajné	Tajné	Dôverné	Vyhradené
<u>Slovenia</u>	Strogo tajno	Tajno	Zaupno	Interno
<u>Spain</u>	Secreto	Reservado	Confidencial	Difusión Limitada
<u>Sri Lanka</u>	අති රහස්‍ය	රහස්‍ය	රහසිගත	සීමාන්විත
<u>Sweden</u>	Kvalificerat Hemlig (KH); Hemlig/Top Secret (H/TS)	Hemlig (H); Hemlig/Secret (H/S)	Hemlig/Confidential (H/C)	Hemlig/Restricted (H/R)
<u>Switzerland</u>		GEHEIM / SECRET	VERTRAULICH / CONFIDENTIEL	INTERN / INTERNE
<u>Taiwan (Republic of China)</u> ^[42]	Top Secret (絕對機密)	Secret (極機密)	Confidential (機密)	no direct equivalent
<u>Tanzania (Swahili)</u>	SIRI KUU	SIRI	STIRI	IMEZULIWA
<u>Thailand</u>	Lap thi sut (ลับที่สุด)	Lap mak (ลับมาก)	Lap (ลับ)	Pok pit (ปกปิด)
<u>Turkey</u>	Çok Gizli	Gizli	Özel	Hizmete Özel
<u>South Africa (English)</u>	Top Secret	Secret	Confidential	Restricted
<u>South Africa (Afrikaans)</u>	Uiters Geheim	Geheim	Vertroulik	Beperk
<u>Ukraine</u>	Цілком таємно	Таємно	Конфіденційно	Для службового користування
<u>United Kingdom</u>	TOP SECRET	SECRET	OFFICIAL-SENSITIVE (formerly CONFIDENTIAL)	OFFICIAL (formerly RESTRICTED)
<u>United States</u>	Top Secret	Secret	Confidential	no direct equivalent
<u>Uruguay</u>	Ultra Secreto	Secreto	Confidencial	Reservado
<u>Vietnam</u>	Tuyệt Mật, 絕密	Tối Mật, 最密	Mật, 密	Phổ Biến Hạn Chế, 普遍限制

Table notes:

- a. Finland uses also the label *Salassa pidettävä*, "to be kept secret" for information that is not classified but must not be revealed on some other basis than national security. (E.g. privacy, trade secrets etc.)

Table source: US Department of Defense (January 1995). "National Industrial Security Program - Operating Manual (DoD 5220.22-M)" (<https://web.archive.org/web/20190727225319/https://apps.dtic.mil/dtic/tr/fulltext/u2/a291750.pdf>) (PDF). pp. B1 - B3 (PDF pages:121–123). Archived from the original (<https://apps.dtic.mil/dtic/tr/fulltext/u2/a291750.pdf>) (PDF) on 27 July 2019. Retrieved 27 July 2019.

Corporate classification

Private corporations often require written confidentiality agreements and conduct background checks on candidates for sensitive positions.^[43] In the U.S. the Employee Polygraph Protection Act prohibits private employers from requiring lie detector tests, but there are a few exceptions. Policies dictating methods for marking and safeguarding company-sensitive information (e.g. "IBM Confidential") are common and some companies have more than one level. Such information is protected under trade secret laws. New product development teams are often sequestered and forbidden to share information about their efforts with un-cleared fellow employees, the original Apple Macintosh project being a famous example. Other activities, such as mergers and financial report preparation generally involve similar restrictions. However, corporate security generally lacks the elaborate hierarchical clearance and sensitivity structures and the harsh criminal sanctions that give government classification systems their particular tone.

Traffic Light Protocol

The Traffic Light Protocol^{[44][45]} was developed by the Group of Eight countries to enable the sharing of sensitive information between government agencies and corporations. This protocol has now been accepted as a model for trusted information exchange by over 30 other countries. The protocol provides for four "information sharing levels" for the handling of sensitive information.

See also

- Economic Espionage Act of 1996 (U.S.)
- Espionage
- Espionage Act of 1917 (U.S.)
- Eyes only
- Government Security Classifications Policy (UK)
- Illegal number

- Information security
- Official Secrets Act (UK, India, Ireland, Malaysia, New Zealand)
- Security of Information Act (Canada)
- State Secrets Privilege (US)
- Wassenaar Arrangement
- WikiLeaks
- UKUSA Agreement
- Five Eyes
- Golden Shield Project

References

1. "United States Cryptologic History: Attack on a Sigint Collector, the U.S.S. Liberty" (https://web.archive.org/web/20121030155345/http://www.nsa.gov/public_info/files/uss_liberty/attack_sigint.pdf) (PDF). NSA.gov. Archived from the original (http://www.nsa.gov/public_info/files/uss_liberty/attack_sigint.pdf) (PDF) on 2012-10-30. Retrieved 2012-11-14.
2. Turner, Stansfield (2005). *Burn Before Reading: Presidents, CIA Directors and Secret Intelligence* (<https://archive.org/details/burnbeforereadin00turn>). New York: Hyperion. ISBN 9780786867820.
3. Goldsmith, Jack (29 September 2010). "Classified Information in Woodward's 'Obama's Wars'" (<https://www.lawfareblog.com/classified-information-woodwards-obamas-wars>). *Lawfare*. Retrieved 5 September 2015.
4. *Random House Webster's Unabridged Dictionary* (2. ed., [Nachdr.] ed.). New York [u.a.]: Random House. 2004. ISBN 0375425993.
5. Defense Technical Information Center (April 1997). "DoD Guide to Marking Classified Documents" (<https://apps.dtic.mil/dois/citations/ADA340216>). dtic.mil.
6. Federation of American Scientists (June 8, 2013). "Chapter 7. Classification Levels" (https://fas.org/sgp/library/quist2/chap_7.html#1). fas.org.
7. Priest, Dana; Arkin, William (19 July 2010). "A hidden world, growing beyond control" (<https://web.archive.org/web/20100720183755/http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control/>). *The Washington Post*. Archived from the original (<http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control/>) on 20 July 2010. Retrieved 5 September 2015.
8. Atomic Energy Commission's Declassification Review of Reports on Human Experiments and the Public Relations and Legal Liability Consequences (https://www.gwu.edu/~nsarchiv/radiation/dir/mstreet/commeet/meet9/brief9/tab_i/br9i2.txt) Archived (https://web.archive.org/web/20130606120441/https://www.gwu.edu/~nsarchiv/radiation/dir/mstreet/commeet/meet9/brief9/tab_i/br9i2.txt) 2013-06-06 at the Wayback Machine, presented as evidence during the 1994 ACHRE hearings.
9. Section 1.7 (1) and (2).
10. "E-PME Enlisted Professional Military Education Reporting Unsecured and Securing Classified Material 4.G.03" (<https://web.archive.org/web/20131029204918/http://www.uscg.mil/petaluma/e-pme/e-pme/apprentice/G-Lessons/4-G-03.pdf>) (PDF). United States Coast Guard. Archived from the original (<http://www.uscg.mil/petaluma/e-pme/e-pme/apprentice/G-Lessons/4-G-03.pdf>) (PDF) on October 29, 2013.
11. George Washington University. "Attachment 2 AR 320-5, Classification of OFC. Army Regulations (1936)" (https://web.archive.org/web/20130713152933/http://www.gwu.edu/~nsarchiv/radiation/dir/mstreet/commeet/meet14/brief14/tab_d/br14d1b.txt). gwu.edu. Archived from the original (http://www.gwu.edu/~nsarchiv/radiation/dir/mstreet/commeet/meet14/brief14/tab_d/br14d1b.txt) on 2013-07-13. Retrieved 2013-06-16.
12. *Government Security Classifications April 2014* (<https://www.gov.uk/government/publications/government-security-classifications>). HMG Cabinet Office. October 2013.
13. Internet. JSK. "OCHRONA INFORMACJI NIEJAWNYCH MIĘDZYNARODOWYCH W SFERZE CYWILNEJ I WOJSKOWEJ – Ochrona informacji niejawnych międzynarodowych w sferze cywilnej i wojskowej – BIP – Agencja Bezpieczeństwa Wewnętrznego" (<http://www.bip.abw.gov.pl/bip/informacje-niejawne-1/ochrona-informacji-nie/153,OCHRONA-INFORMACJI-NIEJAWNYCH-MIEDZYNARODOWYCH-W-SFERZE-CYWILNEJ-I-WOJSKOWEJ.html>). www.bip.abw.gov.pl.
14. "NATO Security Indoctrination" (<https://www.act.nato.int/images/stories/structure/reserve/hqrescomp/nato-security-brief.pdf>) (PDF).
15. Government of Canada, Public Services and Procurement Canada (2018-08-30). "Chapter 9: Security requirements for the North Atlantic Treaty Organization – Industrial Security Manual – Security requirements for contracting with the Government of Canada – Canada.ca" (<https://www.tpsgc-pwgsc.gc.ca/esc-src/msi-ism/chap9-eng.html>). www.tpsgc-pwgsc.gc.ca. Retrieved 2020-09-10.
16. "Decision of 23 September 2013 on the security rules for protecting EU classified information" (<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:274:0001:0050:EN:PDF>). *Official Journal of the European Union*. 15 October 2013. Retrieved 5 September 2015.
17. "306652_CM6554" (http://webarchive.nationalarchives.gov.uk/20050525181742/http://www.fco.gov.uk/Files/kfile/306652_CM6554.pdf) (PDF). Archived from the original (http://www.fco.gov.uk/Files/kfile/306652_CM6554.pdf) (PDF) on 2005-05-25. Retrieved 2012-11-14.
18. "European Centre for Information Policy and Security (ECIPS)" (<https://www.ecips.org/ecips-infosec.pdf>) (PDF). p. 7.

19. *Information security management guidelines* (<https://web.archive.org/web/20130504052957/http://www.protectivesecurity.gov.au/informationsecurity/Documents/Australian%20Government%20classification%20system.pdf>) (PDF), Attorney-General's Department, 18 July 2011, archived from the original (<http://www.protectivesecurity.gov.au/informationsecurity/Documents/Australian%20Government%20classification%20system.pdf>) (PDF) on 4 May 2013, retrieved 14 July 2013
20. Security of Information Act (<http://www.csis.gc.ca/nwsrm/bckgrndrs/bckgrndr12-eng.asp>), Archived (<https://wayback.archive-it.org/all/20080116134930/http://www.csis-scrs.gc.ca/en/newsroom/backgrounders/backgrounder12.asp>) January 16, 2008, at Archive-It
21. "Industrial Security Services – Frequently Asked Questions" (<https://web.archive.org/web/20131120011009/http://ssi-iss.tpsgc-pwgsc.gc.ca/questions/esp-pss-eng.html#q4>). *Public Works and Government Services Canada*. Government of Canada. Archived from the original (<http://ssi-iss.tpsgc-pwgsc.gc.ca/questions/esp-pss-eng.html#q4>) on 20 November 2013. Retrieved 8 November 2012.
22. "ARCHIVED – Non-Insured Health Benefits Program: Privacy Code, 2005 (Appendix II)" (https://web.archive.org/web/20150924043739/http://www.hc-sc.gc.ca/fniah-spnia/pubs/nihb-ssna/_priv/2005_code/index-eng.php#app2). *Health Canada, First Nations and Inuit Health Branch*. 2015. Archived from the original (http://www.hc-sc.gc.ca/fniah-spnia/pubs/nihb-ssna/_priv/2005_code/index-eng.php#app2) on 24 September 2015. Retrieved 5 September 2015.
23. "Security Policy – Manager's Handbook" (https://web.archive.org/web/20050601030559/http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TB_J2/dwnld/spmh_e.rtf). Archived from the original (http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TB_J2/dwnld/spmh_e.rtf) on June 1, 2005.
24. "Archived – Access to Information Guidelines – Confidences of the Queen's Privy Council for Canada" (<https://web.archive.org/web/20151017171415/http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=25487§ion=text%3DTrue>). *Treasury Board of Canada Secretariat*. 2015. Archived from the original (<http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=25487§ion=text%3DTrue>) on 17 October 2015. Retrieved 5 September 2015.
25. Standing Committee of the National People's Congress, "Law on Guarding State Secrets (http://www.gov.cn/banshi/2005-08/21/content_25096.htm)" (中华人民共和国保守国家秘密法), promulgated 1988 and effective 1989.
26. Translation per Human Rights in China, *State Secrets: China's Legal Labyrinth* (<http://hrichina.org/public/contents/41421>), (2007).
27. "Code pénal – Article 413-9" (<http://legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070719&idArticle=LEGIARTI000020933029&dateTexte=20150905>). *Legifrance*. 2009. Retrieved 5 September 2015.
28. [1] (<http://www.csb.gov.hk/hkgcsb/doclib/general.pdf>) Archived (<https://web.archive.org/web/20061201013917/http://www.csb.gov.hk/hkgcsb/doclib/general.pdf>) December 1, 2006, at the Wayback Machine
29. "LCQ3: Equal Opportunities Commission" (https://web.archive.org/web/20081227080400/http://www.hab.gov.hk/en/publications_and_press_releases/press_releases_speeches/equal_opportunities/191103q3.htm). Archived from the original (http://www.hab.gov.hk/en/publications_and_press_releases/press_releases_speeches/equal_opportunities/191103q3.htm) on December 27, 2008.
30. "Penal Code of Romania, art. 150" (<https://legeaz.net/cod-penal-actualizat-2011/art-150-cpen>). Retrieved January 28, 2013.
31. "Law no. 182/2002 on protection of classified information" (http://legislatie.resurse-pentru-democratie.org/182_2002.php). Retrieved January 28, 2013.
32. "Penal Code of Romania, art. 157" (<https://legeaz.net/cod-penal-actualizat-2011/art-157-cpen>). Retrieved January 28, 2013.
33. "Ordinance on the Protection of Federal Information" (<https://www.admin.ch/opc/en/classified-compilation/20070574/index.html>). *Swiss Federal Government*. 1 January 2018. Retrieved 29 January 2020.
34. Diri, Mustafa; Gülçiçek, Mirac (2012). "Türkiye'de Kamu Hizmetinin Görülmesinde Kullanılmakta Olan Gizlilik Derecesi Tanımları : Uygulamadaki Sorunlar ve Çözüm Önerileri" (<https://ms.hmb.gov.tr/uploads/2019/09/26.pdf>) (PDF). *Maliye Dergisi* (in Turkish) (162): 497–537.
35. "Understanding the Security Policy Framework & frequently asked questions" (<http://www.cabinetoffice.gov.uk/spf/faqs.aspx>). Cabinet Office. 1 April 2013. Retrieved 5 September 2015.
36. Aftergood, Steven (August 27, 2014). "Gov't Resists Court Review of State Secrets" (<https://fas.org/blogs/secrecy/2014/08/review-state-secrets/>). *Secrecy News*. Federation of American Scientists. Retrieved 2014-09-26.
37. Ellsberg, Daniel (30 May 2014). "Daniel Ellsberg: Snowden would not get a fair trial – and Kerry is wrong" (<https://www.theguardian.com/commentisfree/2014/may/30/daniel-ellsberg-snowden-fair-trial-kerry-espionage-act>). *The Guardian*. Retrieved 2014-09-26.
38. "DoD Warns Employees of Classified Info in Public Domain – Federation Of American Scientists" (<https://fas.org/blogs/secrecy/2013/06/dod-classified/>).
39. Myers, Steven Lee; Mazzetti, Mark (February 5, 2016). "Agencies Battle Over What Is 'Top Secret' in Hillary Clinton's Emails" (<https://www.nytimes.com/2016/02/06/us/politics/agencies-battle-over-what-is-top-secret-in-hillary-clintons-emails.html>). *The New York Times*.
40. "Secrecy defines Obama's drone war" (https://www.washingtonpost.com/world/national-security/secrecy-defines-obamas-drone-war/2011/10/28/gIQAQPNR5O_story.html). *Washington Post*.
41. "Wet- en regelgeving – Besluit voorschrift informatiebeveiliging rijksdienst – bijzondere informatie – BWBR0016435" (<http://wetten.overheid.nl/BWBR0016435#B>) (in Dutch). *Wetten.overheid.nl*. Retrieved 2013-07-04.
42. "The Classified National Security Information Protection Act" (<http://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=I0060003>). 2003-02-06. Retrieved 2014-03-26.

43. "Employment Background Checks: A Jobseeker's Guide | Privacy Rights Clearinghouse" (<https://web.archive.org/web/20120109003413/http://www.privacyrights.org/fs/fs16-bck.htm>). Privacyrights.org. Archived from the original (<http://www.privacyrights.org/fs/fs16-bck.htm>) on 2012-01-09. Retrieved 2011-12-12.
44. "Development of Policies for Protection of Critical Information Infrastructures" (<http://www.oecd.org/dataoecd/25/10/40761118.pdf>) (PDF). Cecd.ord. Retrieved 2012-11-14.
45. "'Re: OpenSSH security advisory: cbc.adv' – MARC" (<https://marc.info/?l=bugtraq&m=122754275122010&w=2>). Marc.info. Retrieved 2011-12-12.

External links

- Defence Vetting Agency (<http://www.mod.uk/DefenceInternet/AboutDefence/WhatWeDo/SecurityandIntelligence/DVA/DefenceVettingAgency.htm>). Carries out national security checks in the UK.
- Peter Galison, Removing Knowledge (<http://www.fas.harvard.edu/~hsdept/bios/docs/Removing%20Knowledge.pdf>) in *Critical Inquiry* n°31 (Autumn 2004).
- Goldman, Jan, & Susan Maret. *Intelligence and information policy for national security: Key terms and concepts*. Rowman & Littlefield, 2016.
- Lerner, Brenda Wilmoth, & K. Lee Lerner, eds. *Terrorism: Essential primary sources*. Thomson Gale, 2006.
- Los Alamos table of equivalent US and UK classifications (https://web.archive.org/web/20120510051228/http://badge.lanl.gov/uk-usa_classification.shtml)
- Maret, Susan. *On their own terms: A lexicon with an emphasis on information-related terms produced by the U.S. federal government*. [2] (<https://fas.org/sgp/library/maret.pdf>), FAS, 6th ed., 2016.
- *Marking Classified National Security Information* (<https://www.archives.gov/isoo/training/marketing-booklet.pdf>) ISOO booklet.
- The National Security Archive (<http://www.gwu.edu/~nsarchiv/>) – a collection of declassified documents acquired through the FOIA.
- Parliament of Montenegro (<http://www.skupstina.me/index.php?strana=zakoni&id=618>), Law on confidentiality of data. (in Serbian).
- Parliament of Serbia (<http://www.parlament.gov.rs/upload/archive/files/lat/pdf/zakoni/2009/2502-09Lat.zip>), Law on confidentiality of data. (in Serbian).
- U.S. Department of Defense *National Industrial Security Program - Operating Manual (DoD 5220.22-M)* (<https://web.archive.org/web/20110807094949/http://www.dss.mil/isp/odaa/nispom06.html>), explaining rules and policies for handling classified information.

Retrieved from "https://en.wikipedia.org/w/index.php?title=Classified_information&oldid=1030592530"

This page was last edited on 26 June 2021, at 22:32 (UTC).

Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy. Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.