**CLASSIFIE INFORMATION**

**Classified information** is information to which access is restricted by law or regulation to particular classes of people. A formal security clearance is required to handle classified documents or access classified data; the clearance process requires a satisfactory background investigation. There are typically several levels of sensitivity, with differing clearance requirements. This sort of hierarchical system of secrecy is used by virtually every national government.

The purpose of classification is ostensibly to protect information from being used to damage or endanger national security. Classification formalizes what constitutes a "state secret" and accords different levels of protection based on the expected damage the information might cause in the wrong hands.

**Corporate classification**

Private corporations often require written confidentiality agreements and conduct background checks on candidates for sensitive positions. 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.

**Example**

EDS uses three classifications of information. Disclosure of *EDS Limited Distribution* information could cause serious damage to an affected party. Disclosure of *EDS Confidential* information could damage an affected party. Disclosure of *EDS Internal* information (most EDS business information) could be inappropriate or problematic.

**U.S. Government's classification system**

The United States Government classification system is established under Executive Order 13292, the latest in a long series of executive orders on the topic. Issued by President George W. Bush in 2003, Executive Order 13292 lays out the system of classification, declassification and handling of national security information generated by the United States Government and its employees and contractors, as well as information received from other governments.

The desired degree of secrecy about such information is known as its **sensitivity**. Sensitivity is based upon a calculation of the damage to national security that the release of the information would cause. The United States has three levels of classification — **confidential**, **secret**, and **top secret**. Each level of classification indicates an increasing degree of sensitivity. Thus if one holds a top-secret clearance, one is allowed to handle information up to the level of "top-secret" including secret, and confidential information. If one holds a *secret* clearance, one may not then handle *top-secret* information, but may handle *confidential* classified information.

In the United States, information cannot be classified merely because it would be embarrassing; information can only be classified in relationship to protecting national security objectives of the state.

**Accessing Classified Information**

In addition to sensitivity level, information that is classified is restricted in its dissemination based on the "need to know" the information. Having a "top-secret" clearance does not give one access to all documents classified at that level. Rather, information is disseminated based upon sensitivity level *and* the need to know. In addition, dissemination of information is often compartmentalized, requiring special additional clearance requirements. Individuals with access to one type of compartmentalized information may, for that reason alone, be denied access to other compartmentalized information. Individuals who need access to the most sensitive intelligence information hold a "TS/SCI" clearance — Top-Secret/Sensitive Compartmentalized Information. In addition, there are Special Access Programs or "SAPs" that restrict access to all information relating to that program or project to a limited number of pre-approved people.

**Classified Vs. Unclassified Information**

In the U.S. information is called "classified" because it has been assigned one of the three levels, confidential, secret or top secret. Information which is not so labeled is called **unclassified information**. The term **declassified** is used for information which has had its classification removed, and **downgraded** refers to information that has been assigned a lower classification level, but is still classified. Many documents are automatically downgraded and then declassified after some number of years. The U.S. government uses the term **sensitive but unclassified** (SBU) to refer to information that is not confidential, secret or top secret, but whose dissemination is still restricted. Reasons for such restrictions can include export controls, privacy regulations, court orders, and ongoing criminal investigations as well as national security. Information which was never classified is sometimes referred to as "open source" by those who work in classified activities.

**Levels of Classification used by the U.S. Government**

The United States Government classifies information according to the degree which the unauthorized disclosure would damage national security:

**Top secret**

This is the highest security level that is publicly disclosed, and is defined as information which would cause "exceptionally grave damage" to national security if disclosed to the public. Despite public mystique, little information is classified at "Top Secret" when compared to the other levels of classification. Only that which is exceptionally sensitive (weapon design, presidential security information, nuclear-related projects, various intelligence information) is classified at the Top Secret level. Other times, the nature of the gathering method used to obtain the information is what causes the information to be classified "Top Secret", though the information itself may be mundane and unimportant. Examples would be signal interceptions (SIGINT) or Human Intelligence (HUMINT).

**Secret**

The second highest classification. Information is classified secret when its release would cause "serious damage" to national security. Most information that is classified is held at the secret sensitivity.

**Confidential**

The lowest classification level. It is defined as information which would "damage" national security if disclosed.

**Unclassified**

*Unclassified* is not technically a "classification", this is the default, and refers to information which can be released to individuals without a clearance. Information that is unclassified is sometimes restricted in its dissemination as SBU or FOUO, For Official Use Only. For example, the "law enforcement bulletins" often reported by the U.S. media when United States Department of Homeland Security raises the U.S. terror threat level are usually classified as "U//LES" or "Unclassified - Law Enforcement Sensitive." This information is only supposed to be released to Law Enforcement groups (Sheriff, Police, etc.) Because the information is unclassified, however, it is sometimes released to the public as well. Information which is unclassified, but which the government does not believe should be subject to Freedom of Information Act requests is often classified as U//FOUO - Unclassified-For Official Use Only. In addition to FOUO information, information can be categorized according to its availability to be distributed (Distribution D may only be released to approved Department of Defense and Government Contractor persons). Also, the statement of NOFORN (meaning No Foreign Nationals) is applied to any information which may not be released to any non-US Citizen. NOFORN and Distribution statements are often used in conjunction with classified information or alone on SBU information. Documents subject to export controls have a specific warning to that effect.

Use of information restrictions outside the classification system is growing in the U.S. government. In September 2005, J. William Leonard, director of the U.S. National Archives Information Security Oversight Office was quoted in the press as saying "No one individual in government can identify all the controlled, unclassified [categories], let alone describe their rules."

**Restricted**

During and before World War II, the U.S. had a category of classified information called **restricted**, which was below confidential. The U.S. no longer has a restricted classification, but many other nations and NATO do. The U.S. treats "restricted" information it receives from other governments as confidential. The U.S. does use the term **restricted data** in a completely different way to refer to nuclear secrets, as described below.

**Above Top Secret?**

A common question about U.S. classified information is whether a level above Top Secret exists. Looked at one way, the answer is almost certainly no. Executive Order 13292 clearly states the Top Secret is the highest level of classification. If there were some secret Executive Order that created a still higher level, there could be questions of adequate legal notice if someone mishandling that information were to be prosecuted. On the other hand, if a U.S. government agency wants to create a program so secret that the program's name itself is known to only a short list of handpicked individuals who have been recently subjected to the most thorough and intrusive vetting process imaginable, they can do so under the code word and special access provisions of Executive Order 13292. Stringent additional security measures beyond those prescribed for ordinary Top Secret can also be required for the program, which would none the less still be classified at the Top Secret level, but with a code name and other markings added. As a practical matter the distinction is mostly semantic.

**Proper procedure for classifying U.S. government documents**

To be properly classified, a classification authority (an individual charged by the U.S. Government with the right and responsibility to properly determine the level of classification and the reason for classification) must determine the appropriate classification level as well as the reason information is to be classified. A determination must be made as to how and when the document will be declassified and the document marked accordingly. Executive Order 13292 describes the reasons and requirements for information to be classified and declassified. Individual agencies within the government develop guidelines for what information is classified and at what level.

**Protecting classified information**



GSA approved security container.

One of the reasons for classifying state secrets into sensitivity levels is to allow the level of protection to be tailored to risk. The U.S. government specifies in some detail the procedures for protecting classified information. The rooms or buildings where classified material is stored or handled must have a **facility clearance** at the same level as the most sensitive material to be handled. Good quality commercial physical security standards generally suffice for lower levels of classification; at the highest levels, people sometimes have to work in rooms designed like bank vaults (*see* SCIF). The U.S. General Services Administration sets standards for locks and containers used for storage of classified material. The most ubiquitous approved security containers look like heavy duty file cabinets with a combination lock in the middle of one drawer. Advances in methods for defeating mechanical combination locks have lead the U.S. government to switch to electro-mechanical locks that limit the rate at which combinations can be tried out.



Secret cover sheet. Top secret documents have an orange border and confidential documents have blue.

Classified U.S. government documents are typically required to be stamped with their classification on the cover and at the top and bottom of each page. It is often a requirement that each paragraph, title and caption in a document be marked with the highest level of information it contains, usually by placing appropriate initials in parentheses at the beginning (or sometimes end) of the paragraph. It is common to require a brightly-colored cover sheet be affixed to the cover each classified document, to prevent observation of a possibly classified title by someone unauthorized (shoulder surfing) and to remind users to lock up the document when it is unattended. The most sensitive material requires two person integrity, where two cleared individuals are responsible for the material at all times. Approved containers for such material have two separate combination locks, both of which must be opened to access the contents.

There are restrictions on how classified documents can be shipped. Top secret material must go by special courier. Secret material can be sent within the U.S. via registered mail, and confidential material by certified mail. Electronic transmission of U.S. classified information requires the use of National Security Agency approved encryption systems.

Specialized computer operating systems known as trusted operating systems are available for processing classified information. These enforce the classification and labeling rules described above in software. However, as of 2005 they are not considered secure enough to allow uncleared users to share computers with classified activities. Computer networks for sharing classified information, such as SIPRNet, are segregated by the highest sensitivity level they are allowed to transmit.

The destruction of classified documents requires burning, shredding, pulping or pulverizing using approved procedures and must be witnessed and logged. Classified computer data presents special problems. *See* Data remanence

**Classifications and clearances between U.S. government agencies**

In the past, clearances did not necessarily transfer between various U.S. government agencies. For example, an individual cleared for Department of Defense Top Secret had to undergo another investigation before being granted a Department of Energy Q clearance. Agencies are now supposed to honor background investigations by other agencies, if they are still current. Because most security clearances only apply inside the agency where the holder works, if one needs to meet with another agency to discuss classified matters, it is possible and necessary to "pass" one's clearance to the other agency. For example, officials visiting at the White House from other government agencies would pass their clearances to the Executive Office of the President (EOP).

**Categories that are not classifications**

There are also compartments, or "code words", which pertain to specific projects, and are used to more easily manage which individuals require certain information. Code words are not levels of classification themselves, but a person working on project *X* may have the code word for that project added to his file, and then will be given access to the relevant documents. Code words may also label the sources of various documents; for example, there are code words used to indicate that a document may break the cover of intelligence operatives if its content becomes known. The WWII code word *ULTRA* identified information found by decrypting German ciphers, such as the Enigma machine, and which — regardless of its own significance — might inform the Germans that Enigma was broken if they became aware that it was known.

The United States also has a system of "restrictions" which can be added to a document; these are constantly changing, but can include (in abbreviated form) a requirement that the document not be shared with civilian contractor, or not leave a specific room. Some of these include NOFORN, meaning no distribution to foreign nationals, NOCONTRACTOR, meaning no distribution to contract personnel, CRYPTO, meaning methods involved in encrypting communications between government agencies, and CCO, meaning handle by COMINT (communications intelligence) channels only. These restrictions are not classifications in and of themselves, rather, they restrict the dissemination of information within those who have the appropriate clearance level and possibly the "need to know" the information. Remarks such as "eyes only" also limit the restriction. One violating these directives might be guilty of violating a lawful order or mishandling classified information.

**Restricted data**

The Atomic Energy Act of 1954 sets requirements for protection of information about nuclear weapons and special nuclear materials. Such information is "classified from birth," unlike all other sensitive information which must be classified by some authorized individual. Documents containing such information must be marked "RESTRICTED DATA" (RD) or "FORMERLY RESTRICTED DATA" (FRD) in addition to any other classification marking. Persons accessing such data require special clearances from the U.S. Department of Energy. For example, a **Q clearance** is required for access to Top Secret-Restricted Data.

**Critical Nuclear Weapon Design Information**

Critical Nuclear Weapon Design Information (CNWDI) is a U.S. Department of Defense category of TOP SECRET Restricted Data or SECRET Restricted Data that reveals the theory of operation or design of the components of a nuclear weapon. Access to CNWDI is supposed to be kept to the minimum number of individuals needed.

**Naval Nuclear Propulsion Information**

While most Naval Nuclear Propulsion Information is sensitive, it may or may not be classified. The United States Navy recognizes that the public has an interest in environmental, safety, and health information, and that the basic research the Navy carries out can be useful to industry.

**Yankee White Clearance**

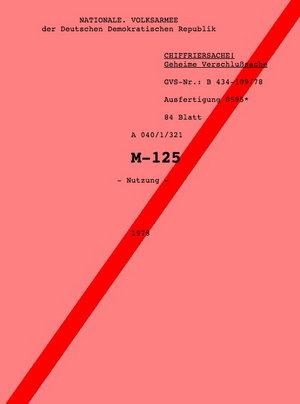
Contrary to popular lore, the Yankee White clearance given to personnel who work directly with the President is not a classification. Individuals having Yankee White clearances undergo extensive background investigation. Yankee White cleared personnel are granted access to any information for which they have a need-to-know, regardless of which organization classified it or at what level. The Yankee White clearance includes a requirement for absolute absence of any foreign influence on the individual. This means they must be a natural-born citizen of the United States, not be or have been married to a person of foreign descent, or have travelled to countries that are considered to be unfriendly to the United States.

**Claims of U.S. government misuse of the classification system**

While the classification of information by the government is not supposed to be used to prevent information from being made public that would be simply embarrassing or reveal criminal acts, it has been alleged that the government routinely misuses the classification system to coverup misdeeds. See, for example, The Pentagon Papers. Many conspiracy theories such as the JFK assassination theories suggest that the government has classified information as top secret that reveals the involvement of agencies such as the CIA.

Various UFO conspiracies mention a level "above top secret" used for UFO design information and related data. They suggest such a classification is intended to apply to information relating to things whose possible existence is to be denied, such as aliens, as opposed to things whose potential existence may be recognized, but for which access to information regarding specific programs would be denied as classified. The existence of an “above top secret” classification is considered by some as unnecessary to keep the existence of aliens a secret, as they say Information at the "Top Secret" level, or any level, can be restricted on the basis of need-to-know. Thus, the U.S. Government could conceal an alien project without having to resort to another level of clearance. The "need to know" would limit the ability to have access to the information. Some suggest that claims of the existence of such a classification level may be based on the mistaken belief that the ‘’levels’’ of classification are themselves classified: As such they feel that books available claiming to contain "above top secret" information on UFOs or remote viewing should arguably be taken with a grain of salt.

**Classifications in other countries**



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 classified material".

Most countries employ some sort of classification system for certain government information. For example, in Canada information which the U.S. would classify SBU is called "protected" and further subcategorized into levels A, B, and C.

New Zealand has an additional grade known as Restricted, which is lower than Confidential. Information with a Restricted classification is not for general dissemination, but is not classified in the strictest sense of the word - it is often used for controlling the release of reports and other documents until it can be done officially. People may be given access to Restricted and Confidential information on the strength of an authorization by their Head of Department, without being subjected to the background vetting associated with Secret and Top Secret clearances. New Zealand's security classifications and the national-harm requirements associated with their use are roughly similar to those of the United States.

Australia also has the classification grade of RESTRICTED. Similar in intent to New Zealand in regards as 'not for general dissemination' it is still a classification level in Federal Government. Background checks are done for this level, although not to the extent as higher classifications.

Australia also has a non-national security based classification system that is used in areas of the Federal Government not directly related to national security matters. This system is used for information whose compromise would not directly threaten the security of the nation, but the release of which could threaten the security or interests of individuals, groups, commercial entities, government business and interests, or the safety of the community

HIGHLY PROTECTED—which broadly corresponds to SECRET in the national security system.

PROTECTED —which broadly corresponds to CONFIDENTIAL in the national security system.

'X'-IN-CONFIDENCE — which broadly corresponds to RESTRICTED in the national security system.

In addition, documents marked 'CABINET-IN-CONFIDENCE', relating to discussions in Federal Cabinet, are treated as PROTECTED.

**Sharing of classified information between countries**

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 which both parties have previously agreed to honor. For example, sensitive information shared amongst NATO allies has four levels of security classification; COSMIC TOP SECRET (CTS), NATO SECRET (NS), NATO CONFIDENTIAL (NC), and NATO RESTRICTED (NR). Another 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 (NSA), or NATO CONFIDENTIAL ATOMAL (NCA).

In cases where the United States wishes to share classified information bilaterally (or multilaterally) with a country that has a sharing agreement, the information is marked "REL" (release) and the three-letter country code. For example, if the U.S. wanted to release classified information to the governments of France, UK, and Canada, it would mark the document "REL FRA, GBR, CAN." Those countries would have to maintain the classification of the document at the level originally classified (TOP-SECRET, SECRET, etc.). The United States has military and national security information sharing agreements with most of its allies.

**Table of equivalent classification markings in various countries**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Country** | **Top Secret** | **Secret** | **Confidential** | **Restricted** |
| Argentina | Estrictamente Secreto | Secreto | Confidencial | Reservado |
| Australia | Top Secret | Secret | Confidential | Restricted |
| Austria | Streng Geheim | Geheim | Verschluss |  |
| Belgium (Flemish) | Zeer Geheim | Geheim | Vertrouwelijk | Beperkte Verspreiding |
| Bolivia | Supersecreto or Muy Secreto | Secreto | Confidencial | Reservado |
| Brazil | Ultra Secreto | Secreto | Confidencial | Reservado |
| Bulgaria | Строго секретно | Секретно | Поверително | За служебно ползване |
| Cambodia | Sam Ngat Bamphot | Sam Ngat Roeung | Art Kambang | Ham Kom Psay |
| Canada | Top Secret | Secret | Confidential | Restricted |
| Chile | Secreto | Secreto | Reservado | Reservado |
| Columbia | Ultrasecreto | Secreto | Reservado | Confidencial |
| Costa Rica | Alto Secreto | Secreto | Confidencial |  |
| Denmark | Yderst Hemmeligt | Hemmeligt | Fortroligt | Tiltjenestebrug |
| Ecuador | Secretisimo | Secreto | Confidencial | Reservado |
| El Savador | Ultra Secreto | Secreto | Confidencial | Reservado |
| Ethiopia | Yemiaz Birtou Mistir | Mistir | Kilkil |  |
| Finland | Erittäin Salainen | Salainen | Luottamuksellinen |  |
| France | Tres Secret | Secret Defense | Confidentiel Defense | Diffusion Restreinte |
| Germany | Streng Geheim | Geheim | VS-Vertraulich | VS-Nur für den Dienstgebrauch |
| Greece | Άκρως Απόρρητον | Απόρρητον | Εμπιστευτικόν | Περιορισμένης Χρήσης |
| Guatemala | Alto Secreto | Secreto | Confidencial | Reservado |
| Haiti | Top Secret | Secret | Confidential | Reserve |
| Hinduras | Super Secreto | Secreto | Confidencial | Reservado |
| Hong Kong | Top Secret | Secret | Confidential | Restricted |
| Hungary | Szigoruan Titkos | Titkos | Bizalmas |  |
| India | Param Gupt | Gupt | Gopniya | Pratibanhst/seemit |
| Indonesia | Sangat Rahasia | Rahasia | Agak Rahasia | Terbatas |
| Iran | Bekoliserri | Serri | Kheil Mahramaneh | Mahramaneh |
| Iraq | Sirri Lil-ghaxah | Sirri | Khass | Mehdoud |
| Ireland | Algjorti | Trunadarmal |  |  |
| Ireland (Gaelic) | An-sicreideach | Sicreideach | Runda | Srianta |
| Israel | Sodi Beyoter סודי ביותר | Sodi סודי | Shamur שמור | Mugbal מוגבל |
| Italy | Segretissimo | Segreto | Riservatissimo | Riservato |
| Japan | Kimitsu | Gokuhi | Hi | Toriaatsukkaichui |
| Jordan | Maktum Jiddan | Maktum | Sirri | Mahdud |
| Korea | I-Kup Bi Mil | II-Kup Bi Mil | III-Kup Bi Mil | Bu Woi Bi |
| Laos | Lup Sood Gnod | Kuam Lup | Kuam Lap | Chum Kut Kon Arn |
| Lebanon | Tres Secret | Secret | Confidentiel |  |
| Mexico | Ultra Secreto | Secreto | Confidencial | Restringido |
| Netherlands | Zeer Geheim | Geheim | Confidentieel or Vertrouwelijk | Dienstgeheim |
| New Zealand | Top Secret | Secret | Confidential | Restricted |
| Nicaragua | Alto Secreto | Secreto | Confidencial | Reservado |
| Norway | Strengt Hemmelig | Hemmelig | Konfidensiell | Begrenset |
| Pakistan (URDU) | Intahai Khufia | Khufia | Sigh-E-Raz | Barai Mahdud Taqsim |
| Paraguay | Secreto | Secreto | Confidencial | Reservado |
| Peru | Estrictamente Secreto | Secreto | Confidencial | Reservado |
| Philippines | Top Secret | Secret | Confidential | Restricted |
| Portugal | Muito Secreto | Secreto | Confidencial | Reservado |
| Republic of Moldova | De importanţă deosebită | Strict Secret | Secret | Pentru uz de serviciu |
| Russia | Совершенно Секретно | Секретно | не подлежит оглашению (Конфиденциально) | Для Служебного Пользования |
| Saudi Arabia | Saudi Top Secret | Saudi Very Secret | Saudi Secret | Saudi Restricted |
| Spain | Maximo Secreto | Secreto | Confidencial | Diffusion Limitada |
| Sweden | Hemlig (thick red border) | Hemlig (thin red border) |  |  |
| Switzerland |  | Geheim | Vertraulich | Armee intern |
| Taiwan | Chichimi | Chimi |  |  |
| Thailand | Lup Tisud | Lup Maag | Lup | Pok Pid |
| Turkey | Cok Gizli | Gizli | Ozel | Hizmete Ozel |
| South Africa (English) | Top Secret | Secret | Confidential | Restricted |
| South Africa(Afrikaans) | Uiters Geheim | Geheim | Vertroulik | Beperk |
| United Arab Republic of Egypt | Jirri Lilghaxeh | SirriKhas | Mehoud | Jidden |
| United Kingdom | Top Secret | Secret | Confidential | Restricted |
| United States | Top Secret | Secret | Confidential |  |
| Uraguay | Ultra Secreto | Secreto | Confidencial | Reservado |
| Viet Nam | Toi-Mat | Mat | Kin | Pho Bien Han Che |

*Source: NISPOM app. B*