**Classified Information in the United States**

From Wikipedia, the free encyclopedia

*For information on practices in other countries, see* [*Classified information*](http://en.wikipedia.org/wiki/Classified_information)*.*

An example of a U.S. [classified document](http://en.wikipedia.org/wiki/Classified_information); page 13 of a [United States](http://en.wikipedia.org/wiki/United_States) [National Security Agency](http://en.wikipedia.org/wiki/National_Security_Agency) report on the [USS Liberty](http://en.wikipedia.org/wiki/USS_Liberty_%28AGTR-5%29) [incident](http://en.wikipedia.org/wiki/USS_Liberty_incident), partially [declassified](http://en.wikipedia.org/wiki/Declassification) and released to the public in July 2003. The original overall classification of the page, "top secret" [code word](http://en.wikipedia.org/wiki/Code_word) UMBRA, is 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.

The [**United States**](http://en.wikipedia.org/wiki/United_States)[**government**](http://en.wikipedia.org/wiki/Federal_government_of_the_United_States)[**classification system**](http://en.wikipedia.org/wiki/Classified_information) is established under [Executive Order 13292](http://en.wikipedia.org/wiki/Executive_Order_13292), the latest in a long series of [executive orders](http://en.wikipedia.org/wiki/Executive_order_%28United_States%29) on the topic. Issued by [President](http://en.wikipedia.org/wiki/President_of_the_United_States) [George W. Bush](http://en.wikipedia.org/wiki/George_W._Bush) in 2003, Executive Order 13292 replaces earlier executive orders on the topic and lays out the system of classification, declassification, and handling of [national security](http://en.wikipedia.org/wiki/National_security) information generated by the U.S. 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](http://en.wikipedia.org/wiki/Information_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 [security clearance](http://en.wikipedia.org/wiki/Security_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 *secret* and *confidential* classified information.

By law, information may not be classified merely because it would be embarrassing or to cover illegal activity; information may only be classified to protect national security objectives.

**Accessing classified information**

Regardless of sensitivity level, dissemination of information that is classified is restricted to those who "need to know" the information. Having a "top-secret" clearance does not give one access to all documents classified at that level. Rather, individuals may access classified information only if they are cleared at information's sensitivity level *and* have a 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" (Top-Secret/Sensitive Compartmented Information) clearance. Special clearances are required for access to cryptographic and nuclear secrets. 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" if it has been assigned one of the three levels: Confidential, Secret, or Top Secret. Information that 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), or [**Sensitive Security Information**](http://en.wikipedia.org/wiki/Sensitive_Security_Information) (SSI), or **Critical Program Information** (CPI), or **For Official Use Only** (FOUO) or **Law Enforcement Sensitive** (LES) 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](http://en.wikipedia.org/wiki/Wassenaar_Arrangement), [privacy](http://en.wikipedia.org/wiki/Privacy) regulations, court orders, and ongoing criminal investigations, as well as national security. Information that was never classified is sometimes referred to as "open source" by those who work in classified activities. **Public Safety Sensitive** (PSS) refers to information that is similar to Law Enforcement Sensitive however could be shared between the various public safety disciplines (Law Enforcement, Fire, and Emergency Medical Services).

**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. There is a misconception that having Top Secret Clearance allows the viewing of all Top Secret documents; however, this is not true. The user of the information must possess (1) the clearance necessary for the sensitivity of the information, as well as (2) a "need to know" the information. For example, all US military pilots are required to obtain a Top Secret Clearance, but they may only access documents directly related to their orders. Secret information might have additional access controls that could prevent someone with a Top Secret classification from seeing it. For example, a document marked "Secret Handle through Comint Channels Only (S-CCO)) would require that the potential reader have a clearance of Secret or higher, but also allowed access to communications intelligence, a subset of [SIGINT](http://en.wikipedia.org/wiki/SIGINT).

**Top secret**

This is the highest security level (**Level 3**) that is publicly disclosed, and is defined as information that would cause "exceptionally grave damage" to [national security](http://en.wikipedia.org/wiki/National_security) if disclosed to the public. Despite the 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. In other cases, 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. An example might be a routine message obtained through [cryptanalysis](http://en.wikipedia.org/wiki/Cryptanalysis) the possession of which might reveal that the code or cipher had been broken.

**Secret**

The second highest classification (**Level 2**). 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 (**Level 1**). 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 that can be released to individuals without a clearance (**Level 0**). Information that is unclassified is sometimes restricted in its dissemination as SBU or FOUO. For example, the "law enforcement bulletins" often reported by the U.S. media when [United States Department of Homeland Security](http://en.wikipedia.org/wiki/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.) only, but because the information is unclassified, however, it is sometimes released to the public as well. Information that is unclassified, but which the government does not believe should be subject to [Freedom of Information Act](http://en.wikipedia.org/wiki/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 personnel). Also, the statement of NOFORN (meaning 'no foreign nationals') is applied to any information that may not be released to any non-U.S. 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.

The restriction of NOFORN no longer applies to Australia or Britain when the matter concerns either a) military operations (including training) in which they are participating or b) the broader war on terror. It was reported that this change took place in July 2004 when President Bush signed a presidential decree changing US national disclosure policy.

Finally, information at one level of classification may be "upgraded by aggregation" to a higher level. For example, a specific technical capability of a weapon system might be classified Secret, but the aggregation of all technical capabilities of the system into a single document could be deemed Top Secret.

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](http://en.wikipedia.org/wiki/U.S._National_Archives) [Information Security Oversight Office](http://en.wikipedia.org/wiki/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."

**Controlled Unclassified Information (CUI)**

One of the [9/11 Commission](http://en.wikipedia.org/wiki/9/11_Commission) findings was that "the government keeps too many secrets. To address this problem, the Commission recommended that `[t]he culture of agencies feeling they own the information they gathered at taxpayer expense must be replaced by a culture in which the agencies instead feel they have a duty . . . to repay the taxpayers' investment by making that information available.' "

Due to 100 plus designations currently in use by the U.S. government for unclassified information, President Bush issued a directive on May 9, 2008, to consolidate these categories into a new category known as [Controlled Unclassified Information](http://en.wikipedia.org/wiki/Controlled_Unclassified_Information) (CUI). CUI will replace categories such as [For Official Use Only](http://en.wikipedia.org/wiki/For_Official_Use_Only) (FOUO), [Sensitive But Unclassified](http://en.wikipedia.org/wiki/Sensitive_But_Unclassified) (SBU) and Law Enforcement Sensitive (LES).

The Presidential memorandum designated the [National Archives](http://en.wikipedia.org/wiki/National_Archives_and_Records_Administration) as responsible for overseeing and managing the implementation of the CUI framework.

The U.S. Congress has taken recent action on this issue. The [U.S. House of Representatives](http://en.wikipedia.org/wiki/U.S._House_of_Representatives) passed the Reducing Information Control Designations Act [H.R. 6576](http://hdl.loc.gov/loc.uscongress/legislation.110hr6576) on September 9, 2008. The bill is now pending before the [U.S. Senate](http://en.wikipedia.org/wiki/U.S._Senate).

**Restricted**

During and before [World War II](http://en.wikipedia.org/wiki/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](http://en.wikipedia.org/wiki/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?**

Books such as [Timothy Good](http://en.wikipedia.org/wiki/Timothy_Good)'s 1988 *Above Top Secret: The Worldwide UFO Cover-Up*, speculate whether such a higher classification level might exist in the U.S. hierarchy.[[*citation needed*](http://en.wikipedia.org/wiki/Wikipedia%3ACitation_needed)] [Executive Order 13292](http://en.wikipedia.org/wiki/Executive_Order_13292), which forms the legal basis for the U.S. classification system, states that "information may be classified at one of the following three levels" with Top Secret as the highest level ([Sec. 1.2](http://en.wikisource.org/wiki/Executive_Order_13292#Sec._1.2._Classification_Levels.)). However, this executive order provides for special-access programs that further restrict access to a small number of individuals and permit additional security measures. ([Sec. 4.3](http://en.wikisource.org/wiki/Executive_Order_13292#Sec._4.3._Special_Access_Programs.)). U.S. law also has special provisions for information related to [cryptography](http://en.wikipedia.org/wiki/Cryptography) ([18 USC 798](http://www.law.cornell.edu/uscode/18/798.html)) and atomic energy (see [#Controls on Atomic Energy Information](http://en.wikipedia.org/wiki/Classified_information_in_the_United_States#Controls_on_Atomic_Energy_Information#Controls_on_Atomic_Energy_Information)).

**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.

The former decision is "original" classification. A great majority of classified documents are created by "derivative" classification. For example, if one piece of information, taken from a SECRET document, is put into a document along with 100 pages of unclassified information, the document, as a whole, will be SECRET. Proper (but often ignored) rules stipulate that every paragraph will bear a classification marking of (U) for UNCLASSIFIED, (C) for CONFIDENTIAL, (S) for SECRET, and (TS) for TOP SECRET. Therefore, in this example, only one paragraph will have the (S) marking. If the page containing that paragraph is double-sided, the page should be marked SECRET on top and bottom of both sides.

An official authorized to do original classification, or an individual following rules in a classification guide, might legitimately, if confusingly, classify a collection of unclassified facts. Assuming that it was known that alien spaceships only appeared as blue-green-blue lights, that knowledge itself would presumably be TOP SECRET, with additional restrictions. If someone aware of that information then collected a set of news articles that only spoke of blue-green-blue light reports, the collection could be classified at the level of the most sensitive information, if the document were titled "Soviet Spy Sightings". That title itself would be classified, and, if the knowledge were TOP SECRET with the REDMEN codeword, there would probably be an unclassified title written (U)Project X(TS-codeword), while the actual title would be written (TS-REDMEN)Accurate Alien Sightings(TS-REDMEN), indicating the title and contents were classified at that level. Note that the unclassified reference only said TS-codeword without revealing the codeword itself, codewords themselves being classified.

A review of classification policies by the [Office of the Director of National Intelligence](http://en.wikipedia.org/wiki/Office_of_the_Director_of_National_Intelligence) aimed at developing a uniform classification policy and a single classification guide that could be used by the entire [U.S. intelligence community](http://en.wikipedia.org/wiki/U.S._intelligence_community) found significant interagency differences that impaired cooperation and performance. The initial ODNI review, completed in January 2008, said in part, "The definitions of 'national security' and what constitutes 'intelligence' — and thus what must be classified — are unclear. ... Many interpretations exist concerning what constitutes harm or the degree of harm that might result from improper disclosure of the information, often leading to inconsistent or contradictory guidelines from different agencies. ... There appears to be no common understanding of classification levels among the classification guides reviewed by the team, nor any consistent guidance as to what constitutes 'damage,' 'serious damage,' or 'exceptionally grave damage' to national security. ... There is wide variance in application of classification levels."

The review recommended that original classification authorities should specify clearly the basis for classifying information, for example, whether the sensitivity derives from the actual content of the information, the source, the method by which it was analyzed, or the date or location of its acquisition. Current policy requires that the classifier be "able" to describe the basis for classification but not that he or she in fact do so.[[8]](http://en.wikipedia.org/wiki/Classified_information_in_the_United_States#cite_note-7#cite_note-7)

**Protecting classified information**

GSA approved security container.

Classified cover sheets. Whenever a classified or protected document is being transmitted, or is in use, it will have a red back sheet and a colored cover sheet:

|  |  |
| --- | --- |
|  -1  | UNCLASSIFIED |
|  0  | FOR OFFICIAL USE ONLY(green) |
|  1  | RESTRICTED(light blue) |
| **CONFIDENTIAL**(blue) |
|  2  | **SECRET**(red) |
|  3  | **TOP SECRET**(orange) |
|  4  | **SCI**(yellow) |

**Facilities and handling**

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](http://en.wikipedia.org/wiki/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](http://en.wikipedia.org/wiki/Bank_vault) (*see* [SCIF](http://en.wikipedia.org/wiki/Sensitive_Compartmented_Information_Facility)). The [U.S. Congress](http://en.wikipedia.org/wiki/U.S._Congress) has such facilities inside the [Capitol Building](http://en.wikipedia.org/wiki/United_States_Capitol), among other Congressional handling procedures for protecting confidentiality.[[9]](http://en.wikipedia.org/wiki/Classified_information_in_the_United_States#cite_note-8#cite_note-8) The U.S. [General Services Administration](http://en.wikipedia.org/wiki/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](http://en.wikipedia.org/wiki/Combination_lock) in the middle of one drawer. Advances in methods for defeating mechanical combination locks have led the U.S. government to switch to electro-mechanical locks that limit the rate at which combinations can be tried out. After so many failed attempts these locks will permanently lock, requiring a locksmith to reset them.

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 that a brightly-colored **cover sheet** be affixed to the cover of each classified document, to prevent observation of a possibly classified title by someone unauthorized ([shoulder surfing](http://en.wikipedia.org/wiki/Shoulder_surfing_%28computer_security%29)) 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](http://en.wikipedia.org/wiki/Registered_mail), and confidential material by [certified mail](http://en.wikipedia.org/wiki/Certified_Mail). Electronic transmission of U.S. classified information requires the use of [National Security Agency](http://en.wikipedia.org/wiki/National_Security_Agency) "[Type 1](http://en.wikipedia.org/wiki/Type_1_encryption)" [approved encryption systems](http://en.wikipedia.org/wiki/NSA_encryption_systems).

Specialized computer [operating systems](http://en.wikipedia.org/wiki/Operating_system) known as [trusted operating systems](http://en.wikipedia.org/wiki/Trusted_operating_system) 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. So if one creates an unclassified document on a Secret device, the resultant data is classified Secret, until it can be manually reviewed. Computer networks for sharing classified information are segregated by the highest sensitivity level they are allowed to transmit, for example, [SIPRNet](http://en.wikipedia.org/wiki/SIPRNet) (Secret) and [JWICS](http://en.wikipedia.org/wiki/JWICS) (Top Secret-SCI).

The destruction of certain types of classified documents requires burning, [shredding](http://en.wikipedia.org/wiki/Paper_shredder), pulping or pulverizing using approved procedures and must be witnessed and logged. Classified computer data presents special problems. *See* [Data remanence](http://en.wikipedia.org/wiki/Data_remanence).

**Lifetime commitment**

When a cleared individual leaves the job or employer for which they were granted access to classified information, they are formally "debriefed" from the program. Debriefing is an administrative process that accomplishes two main goals: it creates a formal record that the individual no longer has access to the classified information for that program; and it reminds the individual of their "lifetime commitment" to protect that information. Typically the individual is asked to sign another [non-disclosure agreement](http://en.wikipedia.org/wiki/Non-disclosure_agreement) (NDA), similar to that which they signed when initially briefed, and this document serves as the formal record. Note that the debriefed individual does not lose their [security clearance](http://en.wikipedia.org/wiki/Security_clearance); they have only surrendered the "need to know" for information related to that particular job.

**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](http://en.wikipedia.org/wiki/United_States_Department_of_Energy) [Q clearance](http://en.wikipedia.org/wiki/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).

The Department of Energy security clearance required to access Top Secret Restricted Data, Formerly Restricted Data, and National Security Information, as well as Secret Restricted Data, is a [Q clearance](http://en.wikipedia.org/wiki/Q_clearance). The lower-level [L clearance](http://en.wikipedia.org/wiki/L_clearance) is sufficient for access to Secret Formerly Restricted Data and National Security Information, as well as Confidential Restricted Data, Formerly Restricted Data, and National Security Information. In practice, access to Restricted Data is granted, on a need-to-know basis, to personnel with appropriate clearances. At one time, a person might hold both a TS and a Q clearance, but that duplication and cost is no longer required. For all practical purposes, TS=Q and S=L.

Contrary to popular lore, the [Yankee White](http://en.wikipedia.org/wiki/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](http://en.wikipedia.org/wiki/Natural-born_citizen) of the United States. Also, have not traveled (save while in government employ and at the instructions of the United States) to countries that are considered to be unfriendly to the United States.

See also the Single Scope Background Investigation below, along with explicit compartmented access indoctrination. Some compartments, especially intelligence-related, may require a [polygraph](http://en.wikipedia.org/wiki/Polygraph) examination, although the reliability of the polygraph is controversial. That the NSA uses it early in the clearance process while the CIA uses it at the end suggests how little agreement there is on the proper use, if any, of the polygraph.

**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 a project 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](http://en.wikipedia.org/wiki/World_War_II) code word [*ULTRA*](http://en.wikipedia.org/wiki/ULTRA) identified information found by decrypting German ciphers, such as the [Enigma machine](http://en.wikipedia.org/wiki/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.

**Sensitive Compartmented Information (SCI) and Special Access Programs (SAP)**

Widely misunderstood as classification levels or specific clearances are the terms "Sensitive Compartmented Information" (SCI) and "Special Access Program" (SAP).

In fact the terms refer to methods of handling certain types of classified information that relate to specific national-security topics or programs whose existence may not be publicly acknowledged, or the sensitive nature of which requires special handling.

The paradigms for these two categories, SCI originating in the intelligence community and SAP in the Department of Defense, addresses two key logistical issues encountered in the day-to-day control of classified information:

* Individuals with a legitimate need-to-know may not be able to function effectively without knowing certain Top Secret facts about their work. However, granting all such individuals a blanket DoD clearance (often known as a "collateral" clearance) at the Top Secret level would be undesirable, not to mention prohibitively expensive.
* The government may wish to limit certain types of sensitive information only to those who work directly on related programs, regardless of the collateral clearance they hold. Thus, even someone with a collateral DoD Top Secret clearance cannot gain access unless it is specifically granted.

SAP and SCI implementation are roughly equivalent, and it is reasonable to discuss their implementation as one topic. For example, SAP material needs to be stored and used in a facility much like the SCIF described below.

Department of Energy information, especially the more sensitive SIGMA categories, may be treated as SAP or SCI.

**Access to compartmented information**

To achieve selective separation of program information while still allowing full access to those working on the program, a separate "compartment," identified by a unique codeword (itself sometimes classified), is created for the information. This entails establishing communication channels, data storage, and work locations ([SCIF](http://en.wikipedia.org/wiki/Sensitive_Compartmented_Information_Facility)—Sensitive Compartmented Information Facility), which are physically and logically separated not only from the unclassified world, but from general Department of Defense classified channels as well. Thus established, all information generated within the compartment is classified according to the general rules above. However, to emphasize that the information is compartmented, all documents are marked with both the classification level and the codeword (and often the caveat "Handle via <compartment name> Channels Only.")

A person is granted access to a specific compartment after the individual has: a) had a [Single Scope Background Investigation](http://en.wikipedia.org/wiki/Single_Scope_Background_Investigation) similar to that required for a collateral Top Secret clearance; b) been indoctrinated (also called "read" or "briefed") into the nature and sensitivity of the compartment; and c) signed a [non-disclosure agreement](http://en.wikipedia.org/wiki/Non-disclosure_agreement) (NDA).

The individual then has access to all information in the compartment, regardless of its classification (and assuming a need-to-know). However, access does not extend to any other compartment; i.e., there is no single "SCI clearance" analogous to DoD collateral Top Secret. In fact, the individual may or may not hold a collateral DoD clearance at any level; a separate process must be initiated to obtain those. In practice, however, an individual granted SCI access would certainly qualify for a Secret clearance, and likely a Top Secret clearance; obtaining these, however, represents additional cost to the individual's employer, so it is not always pursued.

**Groups of compartmented information**

SAPs are subdivided into three further groups [[1]](http://www.fas.org/sgp/library/nispom.htm). There is no public reference to whether SCI is divided in the same manner, but news reports reflecting that only the "Big 8" members of Congress are briefed on certain intelligence activities, it may be assumed that similar rules apply for SCI. The groups are

* Acknowledged: appears as a line item as "classified project" or the equivalent in the US budget, although details of its content are not revealed. The budget element will associate the SAP with an organization or major command, such as the Navy or Strategic Command
* Unacknowledged: no reference in the published budget; its funding is hidden in another entry, often called the "black budget". The appropriate Congressional committees, however, are briefed on the nature of the SAP and approve it.
* Waived: no mention in the budget, and briefed only to the "Big 8" members of Congress: Speaker of the House, House Minority Leader, Senate Majority and Minority Leaders, and the Chairman and Ranking Minority Members of the appropriate committees.

Examples of SCI topics are sensitive intelligence activities, nuclear secrets, and stealth technology. One or more compartments may be created for each area, and each of these compartments may contain multiple programs or projects (*e.g.,* a specific reconnaissance satellite, ICBM, or stealth aircraft), themselves with their own codenames.

Specific compartmented programs will have their own specific rules. For example, it is standard that no person is allowed unaccompanied access to a nuclear weapon, or to command & control systems for nuclear weapons. Personnel with nuclear-weapons access are under the [Personnel Reliability Program](http://en.wikipedia.org/wiki/Personnel_Reliability_Program).

Some highly sensitive SAP or SCI programs may also use the "no lone zone" method (that is, a physical location into which no one is allowed to enter unaccompanied) described for nuclear weapons.

**Handling caveats**

The United States also has a system of restrictive caveats that 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. 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.

For ease of use, codewords or abbreviations have been adopted that can be included in the summary classification marking (header/footer) to enable the restrictions to be identified at a glance. Some of these codes are:

* NOFORN — Distribution to non-US citizens is prohibited, regardless of their clearance or access permissions.
* RESTRICTED — Distribution to non-US citizens or those holding an interim clearance is prohibited; certain other special handling procedures apply.
* NOCONTRACTOR — Distribution to contractor personnel (non-US-government employees) is prohibited, regardless of their clearance or access permissions.
* REL TO <country code(s)> — Distribution to citizens of the countries listed is permitted, providing they have appropriate accesses and need to know. Example: "REL TO AUS, GBR, CAN, NZ" indicates that the information may be shared with appropriate personnel from Australia, Great Britain, Canada, and New Zealand.
* <nn>X<m> — Information is exempt from automatic declassification (after the statutory default of 10 years) for exemption reason <m>, and declassification review shall not be permitted for <nn> years (up to 25). Example: "25X1" indicates the information must remain classified for 25 years, since it pertains to intelligence activities, sources, or methods (reason "1"). Nine exemption categories are listed in Sec. 3.3 of [Executive Order 13292](http://en.wikipedia.org/wiki/Executive_Order_13292).
* ORCON — Originator controls dissemination and/or release of the document.

Classification level and caveats are typically separated by "//" in the summary classification marking. For example, the final summary marking of a document might be:

SECRET//<compartment name>//NOFORN//ORCON//25X1

**Controls on Atomic Energy Information**

The [Atomic Energy Act of 1954](http://en.wikipedia.org/wiki/Atomic_Energy_Act_of_1954) sets requirements for protection of information about [nuclear weapons](http://en.wikipedia.org/wiki/Nuclear_weapon) and [special nuclear materials](http://en.wikipedia.org/wiki/Special_nuclear_material). Such information is "[classified from birth](http://en.wikipedia.org/wiki/Born_secret)," unlike all other sensitive information, which must be classified by some authorized individual. However, authorized classifiers still must determine whether documents or material are classified or restricted.

The [U.S. Department of Energy](http://en.wikipedia.org/wiki/U.S._Department_of_Energy) recognizes two types of Restricted Data:

* **Restricted Data.** Data concerning the design, manufacture, or utilization of atomic weapons; production of special nuclear material; or use of special nuclear material in the production of energy.
* **Formerly Restricted Data.** Classified information jointly determined by the DOE and the Department of Defense to be related primarily to the military utilization of atomic weapons, and removed from the Restricted Data category.

Documents containing such information must be marked "RESTRICTED DATA" (RD) or "FORMERLY RESTRICTED DATA" (FRD) in addition to any other classification marking. Restricted Data and Formerly Restricted Data are further categorized as Top Secret, Secret, or Confidential.

**Sigma Categories and Critical Nuclear Weapon Design Information**

RESTRICTED DATA contains further compartments. The Department of Energy establishes a list of "SIGMA Categories"[[16]](http://en.wikipedia.org/wiki/Classified_information_in_the_United_States#cite_note-15#cite_note-15) for more fine-grained control than RESTRICTED DATA. [Critical Nuclear Weapon Design Information](http://en.wikipedia.org/wiki/Critical_Nuclear_Weapon_Design_Information) (CNWDI) (colloquially pronounced *"Sin-Widdy"*) reveals the theory of operation or design of the components of a nuclear weapon. As such, it would be SIGMA 1 or SIGMA 2 ([sigmas](http://en.wikipedia.org/wiki/Classified_information_in_the_United_States#CITEREF_sigmas#CITEREF_sigmas)) material, assuming laser fusion is not involved in the information.

Access to CNWDI is supposed to be kept to the minimum number of individuals needed. In written documents, paragraphs containing the material, assuming it is TOP SECRET, would be marked (TS)(RD)(N), where (N) is a shorter way of writing CNWDI. SIGMA information of especial sensitivity may be handled much like SAP or SCI material (q.v.)

**Naval Nuclear Propulsion Information**

While most [Naval Nuclear Propulsion Information](http://en.wikipedia.org/wiki/Naval_Nuclear_Propulsion_Information) is sensitive, it may or may not be classified. However, since naval reactors normally run with highly enriched fuel and, as opposed to most other reactors, might possibly be driven into an uncontrolled fission reaction, design details will almost certainly be classified. The [United States Navy](http://en.wikipedia.org/wiki/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.

**Sharing of classified information with other countries**

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 (or TRI-Graph).

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 TO CAN, FRA, GBR." There are also group releases, such as NATO or [UKUSA](http://en.wikipedia.org/wiki/UKUSA). Those countries would have to maintain the classification of the document at the level originally classified (TOP-SECRET, SECRET, etc.).

In practice, documents may be marked NOFORN EXCEPT (Country or countries).

**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 cover up misdeeds. See, for example, [The Pentagon Papers](http://en.wikipedia.org/wiki/The_Pentagon_Papers). Many conspiracy theories such as the [JFK assassination](http://en.wikipedia.org/wiki/JFK_assassination) theories suggest that the government has classified information as top secret that reveals the involvement of agencies such as the [CIA](http://en.wikipedia.org/wiki/Central_Intelligence_Agency).

Steven Aftergood, director of the Project on Government Secrecy at the [Federation of American Scientists](http://en.wikipedia.org/wiki/Federation_of_American_Scientists), and an expert on classified information, notes that "... inquiring into classified government information and disclosing it is something that many national security reporters and policy analysts do, or try to do, every day. And with a few narrow exceptions — for particularly sensitive types of information — courts have determined that this is not a crime." Aftergood notes that "The universe of classified information includes not only genuine national security secrets, such as confidential intelligence sources or advanced military technologies, but an endless supply of mundane bureaucratic trivia, such as 50-year-old intelligence budget figures, as well as the occasional crime or cover-up."

Various [UFO](http://en.wikipedia.org/wiki/Unidentified_flying_object) 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 British government, for example, denied for several decades that they were either involved or interested in 'UFO' sightings. However, in 2008, the government revealed they have monitored UFO activity for at least the past 30 years.

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 for that matter, can be restricted on the basis of [need to know](http://en.wikipedia.org/wiki/Need_to_know). Thus, the U.S. Government could conceal an alien project without having to resort to another level of clearance, as "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 unsubstantiated 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](http://en.wikipedia.org/wiki/Remote_viewing) should arguably be [taken with a grain of salt](http://en.wikipedia.org/wiki/Pinch_of_salt).

Without making a judgment on if such classifications have been used for space aliens, it is a reality that even the name of some compartments was classified, and certainly the meaning of the code name. In the cited document, a (S) means the material it precedes is SECRET and (TS) means TOP SECRET. According to the Department of Defense directive. "the fact of" the existence of [NRO](http://en.wikipedia.org/wiki/National_Reconnaissance_Office) was at the SECRET level for many years, and the fact of and the actual phrase "National Reconnaissance Program" (see Paragraph II). Paragraph V(a) is largely redacted, but the introduction to the documents clarifies [see Document 19] that refers to the now-cancelled BYEMAN code word and control channel for NRO activities. BYEMAN, the main NRO compartment, was classified as a full word, although the special security offices could refer, in an unclassified way, to "B policy".

**References**

1. [**^**](http://en.wikipedia.org/wiki/Classified_information_in_the_United_States#cite_ref-0#cite_ref-0) William D. Gerhard and Henry W. Millington, [*Attack on a Sigint Collector, the U.S.S. Liberty*](http://www.nsa.gov/liberty/liber00010.pdf), 1981
2. [**^**](http://en.wikipedia.org/wiki/Classified_information_in_the_United_States#cite_ref-1#cite_ref-1) ["Executive Order 12958 - Classified National Security Information, as Amended"](http://www.archives.gov/isoo/policy-documents/eo-12958-amendment.html). [Information Security Oversight Office](http://en.wikipedia.org/wiki/Information_Security_Oversight_Office) of [The National Archives](http://en.wikipedia.org/wiki/National_Archives_and_Records_Administration). <http://www.archives.gov/isoo/policy-documents/eo-12958-amendment.html>. Retrieved on 2008-04-17.
3. [**^**](http://en.wikipedia.org/wiki/Classified_information_in_the_United_States#cite_ref-2#cite_ref-2) Michael J. Sniffen, "[Report: Gov't Secrecy Grows, Costs More](http://www.ftimes.com/main.asp?SectionID=1&SubSectionID=1&ArticleID=29262&TM=68081.09)," Associated Press, September 5, 2005 (accessed December 15, 2006)
4. [**^**](http://en.wikipedia.org/wiki/Classified_information_in_the_United_States#cite_ref-3#cite_ref-3) (July 30, 2008) "[House Report 110-810 - REDUCING INFORMATION CONTROL DESIGNATIONS ACT](http://thomas.loc.gov/cgi-bin/cpquery/T?&report=hr810&dbname=110&)". *BACKGROUND AND NEED FOR LEGISLATION*, [Washington, D.C.](http://en.wikipedia.org/wiki/Washington%2C_D.C.): [Congress of the United States](http://en.wikipedia.org/wiki/Congress_of_the_United_States). Retrieved on [October 21, 2008](http://en.wikipedia.org/w/index.php?title=October_21,_2008&action=edit&redlink=1).
5. [**^**](http://en.wikipedia.org/wiki/Classified_information_in_the_United_States#cite_ref-4#cite_ref-4) Casteli, Elise (January 22, 2008), "[New policy expected soon for sensitive information](http://www.federaltimes.com/index.php?S=3323622)", *Federal Times*, <http://www.federaltimes.com/index.php?S=3323622>
6. [**^**](http://en.wikipedia.org/wiki/Classified_information_in_the_United_States#cite_ref-5#cite_ref-5) The Office of the White House (May 9, 2008). [*Memorandum For The Heads Of Executive Departments And Agencies - Designation and Sharing of Controlled Unclassified Information (CUI)*](http://www.whitehouse.gov/news/releases/2008/05/20080509-6.html). [Press release](http://en.wikipedia.org/wiki/News_release). <http://www.whitehouse.gov/news/releases/2008/05/20080509-6.html>. Retrieved on October 21, 2008.
7. [**^**](http://en.wikipedia.org/wiki/Classified_information_in_the_United_States#cite_ref-6#cite_ref-6) The National Archives (May 22, 2008). [*Archivist of the United States Establishes "Controlled Unclassified Information Office"*](http://www.archives.gov/press/press-releases/2008/nr08-107.html). [Press release](http://en.wikipedia.org/wiki/News_release). <http://www.archives.gov/press/press-releases/2008/nr08-107.html>. Retrieved on October 21, 2008.
8. [**^**](http://en.wikipedia.org/wiki/Classified_information_in_the_United_States#cite_ref-7#cite_ref-7) ["Intelligence Community Classification Guidance: Findings and Recommendations Report"](http://www.fas.org/sgp/othergov/intel/class.pdf) (PDF). Office of the Director of National Intelligence. January 2008. <http://www.fas.org/sgp/othergov/intel/class.pdf>. Retrieved on 2008-04-10.
9. [**^**](http://en.wikipedia.org/wiki/Classified_information_in_the_United_States#cite_ref-8#cite_ref-8) Kaiser, Frederick M. (2008-05-27). ["Protection of Classified Information by Congress: Practices and Proposals"](http://www.fas.org/sgp/crs/secrecy/RS20748.pdf) (PDF). [Congressional Research Service](http://en.wikipedia.org/wiki/Congressional_Research_Service). <http://www.fas.org/sgp/crs/secrecy/RS20748.pdf>. Retrieved on 2008-06-22.
10. [**^**](http://en.wikipedia.org/wiki/Classified_information_in_the_United_States#cite_ref-9#cite_ref-9) Berkowtiz, Howard C. (2008-05-26). ["Unexpected consequences of compartmented security physical facilities"](http://en.citizendium.org/wiki/Compartmented_control_system/Signed_Articles). [Citizendium](http://en.wikipedia.org/wiki/Citizendium). <http://en.citizendium.org/wiki/Compartmented_control_system/Signed_Articles>. Retrieved on 2008-06-30.
11. [**^**](http://en.wikipedia.org/wiki/Classified_information_in_the_United_States#cite_ref-10#cite_ref-10) Los Alamos National Laboratory, [Clearance Processing](http://www.lanl.gov/security/clearances/index.shtml), accessed December 15, 2006
12. [**^**](http://en.wikipedia.org/wiki/Classified_information_in_the_United_States#cite_ref-11#cite_ref-11) [The Football](http://www.globalsecurity.org/wmd/systems/nuclear-football.htm), GlobalSecurity.org
13. [**^**](http://en.wikipedia.org/wiki/Classified_information_in_the_United_States#cite_ref-12#cite_ref-12) ["Director of Central Intelligence Directive 1/7: Security Controls on the Dissemination of Intelligence Information"](http://www.fas.org/irp/offdocs/dcid1-7.html). June 1998. <http://www.fas.org/irp/offdocs/dcid1-7.html>. Retrieved on 2000-09-30.
14. [**^**](http://en.wikipedia.org/wiki/Classified_information_in_the_United_States#cite_ref-13#cite_ref-13) ["Department of Defense Overprint to the National Industrial Security Program"](http://fas.org/sgp/library/nispom_dod_overprint.pdf) (PDF). February 1995. <http://fas.org/sgp/library/nispom_dod_overprint.pdf>.
15. [**^**](http://en.wikipedia.org/wiki/Classified_information_in_the_United_States#cite_ref-14#cite_ref-14) Los Alamos National Laboratory, [*Guide to Portion Marking Documents and Material*, Appendix B, Definitions](http://www.hr.lanl.gov/SCourses/All/PortionMarking/define.htm), accessed December 15, 2006
16. [**^**](http://en.wikipedia.org/wiki/Classified_information_in_the_United_States#cite_ref-15#cite_ref-15) ["[no title, apparent extract from University of California laboratory security briefing](http://labs.ucop.edu/internet/security/brief04/docs/sigmas.pdf)"] (PDF). University of California. n.d.. <http://labs.ucop.edu/internet/security/brief04/docs/sigmas.pdf>. Retrieved on 2007-09-30.
17. [**^**](http://en.wikipedia.org/wiki/Classified_information_in_the_United_States#cite_ref-16#cite_ref-16) Aftergood, Steven (Spring, 2008). ["Classified Documents: Secrecy vs. Citizenship"](http://www.nieman.harvard.edu/reports/08-1NRspring/p19-aftergood.html). Nieman Foundation for Journalism at [Harvard University](http://en.wikipedia.org/wiki/Harvard_University). <http://www.nieman.harvard.edu/reports/08-1NRspring/p19-aftergood.html>. Retrieved on 2008-04-16.
18. [**^**](http://en.wikipedia.org/wiki/Classified_information_in_the_United_States#cite_ref-17#cite_ref-17) ["British Ministry of Defense UFO Archives"](http://ufos.nationalarchives.gov.uk). <http://ufos.nationalarchives.gov.uk>.
19. [**^**](http://en.wikipedia.org/wiki/Classified_information_in_the_United_States#cite_ref-18#cite_ref-18) ["DoD Directive TS-5105.23 [title originally classified](http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB35/08-01.htm) (S) National Reconnaissance Office"]. 1964-03-27. <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB35/08-01.htm>.
20. [**^**](http://en.wikipedia.org/wiki/Classified_information_in_the_United_States#cite_ref-19#cite_ref-19) ["The NRO Declassified"](http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB35/index.html). 2000-09-27. <http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB35/index.html>.

**Additional sources**

* [Security Classified and Controlled Information: History, Status, and Emerging Management Issues](http://www.fas.org/sgp/crs/secrecy/RL33494.pdf), Congressional Research Service, January 2, 2008
* [Executive Order 13292](http://en.wikipedia.org/wiki/Executive_Order_13292) [text at WikiSource](http://en.wikisource.org/wiki/Executive_Order_13292)
* [DoD 5220.22-M](http://www.dss.mil/isec/nispom.htm) [National Industrial Security Program](http://en.wikipedia.org/wiki/National_Industrial_Security_Program) Operating Manual (NISPOM)
* [400 Series DOE Directives by Number](http://www.directives.doe.gov/cgi-bin/explcgi?4??+%3Cin%3E+series;maxdocs=300;APP=onixdoe;collection=neword,newguide,newmanual,newpolicy,newnotice;UP=current.html;INTERFACE=1WINDOW) The 400 series of directives is where DOE keeps most security and classification related items.
* [Atomic Energy Act of 1954](http://en.wikipedia.org/wiki/Atomic_Energy_Act_of_1954) 42 USC 2168 [[2]](http://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0980/ml022200075-vol1.pdf#pagemode=bookmarks&page=14) or [[3]](http://assembler.law.cornell.edu/uscode/)
* [Espionage Act](http://en.wikipedia.org/wiki/Espionage_Act) 18 USC 793, 794, 798 [[4]](http://assembler.law.cornell.edu/uscode/)
* [Designation and Sharing of Controlled Unclassified Information (CUI)](http://www.fas.org/sgp/bush/cui.html), Presidential Memo of May 7, 2008

**See also**

* [Classified information](http://en.wikipedia.org/wiki/Classified_information) for international usage
* [Controlled Cryptographic Item](http://en.wikipedia.org/wiki/Controlled_Cryptographic_Item)
* [Espionage Act](http://en.wikipedia.org/wiki/Espionage_Act)
* [Executive Order 13292](http://en.wikipedia.org/wiki/Executive_Order_13292)
* [FAA 1600.2](http://en.wikipedia.org/wiki/FAA_1600.2)
* [Information Security Oversight Office](http://en.wikipedia.org/wiki/Information_Security_Oversight_Office)
* [Invention Secrecy Act](http://en.wikipedia.org/wiki/Invention_Secrecy_Act)
* [List of U.S. security clearance terms](http://en.wikipedia.org/wiki/List_of_U.S._security_clearance_terms)
* [Naval Nuclear Propulsion Information](http://en.wikipedia.org/wiki/Naval_Nuclear_Propulsion_Information)
* [*Secrecy News*](http://en.wikipedia.org/wiki/Secrecy_News), a newsletter that covers U.S. classification policy
* [SCIF](http://en.wikipedia.org/wiki/Sensitive_Compartmented_Information_Facility) (Sensitive Compartmented Information Facility)
* [Work of the United States Government](http://en.wikipedia.org/wiki/Work_of_the_United_States_Government)
* [United States v. Reynolds](http://en.wikipedia.org/wiki/United_States_v._Reynolds)