**Security Clearance**

From Wikipedia, the free encyclopedia

A **security clearance** is a status granted to individuals allowing them access to [classified information](http://en.wikipedia.org/wiki/Classified_information) (state or organizational [secrets](http://en.wikipedia.org/wiki/Secret)) or to [restricted areas](http://en.wikipedia.org/wiki/Exclusion_zone), after completion of a thorough [background check](http://en.wikipedia.org/wiki/Background_check). The term "security clearance" is also sometimes used in private organizations that have a formal process to [vet](http://en.wikipedia.org/wiki/Vetting) employees for access to sensitive information. A clearance by itself is normally not sufficient to gain access; the organization must also determine that the cleared individual [needs to know](http://en.wikipedia.org/wiki/Need_to_know) specific information. No one is supposed to be granted automatic access to classified information solely because of rank, position, or a security clearance.

**Canada**

*This section deals with access to sensitive government information. '****Police Security Certificate'*** *or similar terminology for immigration or employment purposes usually refers to* [*Criminal Record Check*](http://en.wikipedia.org/wiki/Criminal_record#Screening) *and* ***Transportation Security Clearance Program****, operated by* [*Transport Canada*](http://en.wikipedia.org/wiki/Transport_Canada) *mandatory for marine and airport workers for the purpose of entering restricted area are not within the topic in this article.*

Further information: [Information Classification in Canada](http://en.wikipedia.org/wiki/Classified_information#Canada)

**Background**

Government classified information is governed by the [Treasury Board](http://en.wikipedia.org/wiki/Treasury_Board) Standard on Security Screening, the [*Security of Information Act*](http://en.wikipedia.org/wiki/Security_of_Information_Act) and [*Privacy Act*](http://en.wikipedia.org/wiki/Privacy_Act_(Canada)). Only those that are deemed to be loyal and reliable, and have been cleared are allowed to access sensitive information. The policy was most recently revised on October 20, 2014.

Checks include basic demographic and criminal record checks for all levels, and, depending on an individual appointment's requirements, credit checks, loyalty, and field checks might be conducted by the [RCMP](http://en.wikipedia.org/wiki/Royal_Canadian_Mounted_Police) and/or [CSIS](http://en.wikipedia.org/wiki/Canadian_Security_Intelligence_Service).

Clearance is granted, depending on types of appointment, by individual Federal government departments or agencies or by private company security officers. Those who have contracts with [Public Works and Government Services Canada](http://en.wikipedia.org/wiki/Public_Works_and_Government_Services_Canada) are bound by the Industrial Security Program, a sub-set of the GSP.

To access [designated information](http://en.wikipedia.org/wiki/Classified_information#Canada), one must have at least standard reliability status (see Hierarchy below). Reliability checks and assessments are conditions of employment under the *Public Service Employment Act*, and, thus, all Government of Canada employees have at least reliability status screening completed prior to their appointment. However, Government employees by [Order-in-council](http://en.wikipedia.org/wiki/Order-in-council) are not subjected to this policy.

Clearances at the reliability status and secret levels are valid for 10 years, whereas top secret is valid for 5 years. However, departments are free to request their employees to undergo security screening any time for cause. Because security clearances are granted by individual departments instead of one central government agency, clearances are inactivated at the end of appointment or when an individual transfers out of the department. The individual concerned can then apply to reactivate and transfer the security clearance to his/her new position.

**Hierarchy**

Three levels of personnel screening exist, with two sub-screening categories:

Standard screenings are completed for individuals without law enforcement, security and intelligence functions with the government, whereas Enhanced screenings are for individuals with law enforcement, security and intelligence functions, or access to those data or facilities.

**Security screening**

Individuals who need to have RS because of their job or access to federal government assets will be required to sign the *Personnel Screening, Consent and Authorization Form* (TBS/SCT 330-23e).

* **Reliability Status, Standard** (RS)
  + Reliability checks are done by verifying personal data, criminal records check, credit check, educational, and professional qualifications, data on previous employment and references.
  + This level of clearance will grant the right to access designated documents with markings of Protected A & B information/assets on a [need-to-know](http://en.wikipedia.org/wiki/Need_to_know) basis. It is mandatory for individuals when the duties or tasks of a position or contract necessitate access to protected information and assets, regardless of the duration of an assignment.
* **Reliability status, Enhanced** (ERS)
  + In addition to the Reliability Status, Standard checks, open-source checks, and security questionnaire or interview are required.
  + This level of clearance will grant the right to access designated documents with markings of Protected A, B & C information/assets on a [need-to-know](http://en.wikipedia.org/wiki/Need_to_know) basis.

**Security clearances**

Individuals who require access to more sensitive information (or access to sensitive federal government sites and/or assets) because of their job will be required to sign the *Security Clearance Form* (TBS/SCT 330-60e). There are two levels of clearance:

* **Secret**
  + Secret clearance is only granted after a reliability status is cleared, with a positive CSIS security assessment.
  + This level of clearance will grant the right to access designated and classified information up to Secret level on a need-to-know basis. Department Heads have the discretion to allow for an individual to access Top Secret-level information without higher-level clearance on a case-to-case basis.
  + Only those with a Secret clearance, with enhanced screening have access to Protected C information.
* **Top Secret**
  + In addition to the checks at the Secret level, foreign travels, assets, and character references must be given. Field check will also be conducted prior to granting the clearance.
  + This level of clearance will grant the right to access all designated and classified information on a need-to-know basis.

**Site access**

Two additional categories called "Site Access Status" and "Site Access Clearance" exist not for access to information purposes but for those that require physical access to sites or facilities designated by [CSIS](http://en.wikipedia.org/wiki/Canadian_Security_Intelligence_Service) as areas "reasonably be expected to be targeted by those who engage in activities constituting threats to the security of Canada". Designated areas include [Government Houses](http://en.wikipedia.org/wiki/Government_Houses_of_Canada), official residences of government officials, [Parliament](http://en.wikipedia.org/wiki/Parliament_Hill#Parliament_buildings), [nuclear facilities](http://en.wikipedia.org/wiki/List_of_Canadian_nuclear_facilities), airport restricted areas, maritime ports, and any large-scale events that are sponsored by the federal government (e.g., [2010 Winter Olympics](http://en.wikipedia.org/wiki/2010_Winter_Olympics)).

Where reliability is the primary concern, a site access status screening (similar to a reliability status, standard screening) is conducted ; where loyalty to Canada is the primary concern, a site access clearance (similar to a Secret clearance screening) is required. They are both valid for 10 years.

**Legal**

Prior to granting access to information, an individual who has been cleared must sign a *Security Screening Certificate and Briefing Form* (TBS/SCT 330-47), indicating their willingness to be bound by several [Acts of Parliament](http://en.wikipedia.org/wiki/Acts_of_Parliament) during and after their appointment finishes. Anyone who has been given a security clearance and releases designated/classified information without legal authority is in breach of trust under section 18(2) of the [*Security of Information Act*](http://en.wikipedia.org/wiki/Security_of_Information_Act) with a punishment up to 2 years in jail. Those who have access to Special Operational Information are held to a higher standard. The release of such information is punishable by law, under section 17(2) of the [*Security of Information Act*](http://en.wikipedia.org/wiki/Security_of_Information_Act), liable to imprisonment for life.

The [Criminal Code of Canada](http://en.wikipedia.org/wiki/Criminal_Code_of_Canada), Section 750 (3) states that no person convicted of an offence under Section 121 (frauds on the Government), Section 124 (selling or purchasing office), Section 380 (Fraud - if directed against Her Majesty) or Section 418 (selling defective stores to Her Majesty), has, after that conviction, the capacity to contract with Her Majesty or to receive any benefits under a contract between Her Majesty and any other person or to hold office under Her Majesty unless a pardon has been granted. (This effectively prohibits granting of a Reliability Status to any such individual.)

**United Kingdom**

Further information: [UK Security clearance](http://en.wikipedia.org/wiki/Classified_information_in_the_United_Kingdom#Security_clearance)

Clearance is checked at six levels, depending on the classification of materials that can be accessed — Baseline Personnel Security Standard (BPSS), Counter-Terrorist Check (CTC), Security Check (SC) and Developed Vetting (DV). Security Check allows an individual long-term unsupervised access to protectively-marked SECRET material, whilst for TOP SECRET Developed Vetting is required. All Officers and some specialist trades within the British Armed Forces are cleared to SC to enable them to carry out their jobs. Further to this, in the Royal Corps of Signals, all operators in special handling communications cells and SNCOs holding the appointment [Foreman of Signals](http://en.wikipedia.org/wiki/Foreman_of_Signals) or [Yeoman of Signals](http://en.wikipedia.org/wiki/Yeoman_of_Signals) are required to be DV cleared. Additionally, all appointments within the Intelligence Corps are DV cleared. Those with security clearance are commonly required to sign a statement to the effect that they agree to abide by the restrictions of the [Official Secrets Act](http://en.wikipedia.org/wiki/Official_Secrets_Act). This is popularly referred to as "signing the Official Secrets Act". Signing this has no effect on which actions are legal, as the act is a law, not a contract, and individuals are bound by it whether or not they have signed it. Signing it is intended more as a reminder to the person that they are under such obligations. To this end, it is common to sign this statement both before and after a period of employment that involves access to secrets.

**History**

After the [United States](http://en.wikipedia.org/wiki/United_States) entered into [World War II](http://en.wikipedia.org/wiki/World_War_II), Britain changed its security classifications to match those of America. Previously, classifications had included the top classification "Most Confidential", but it soon became apparent that the United States did not fully understand British classifications, and classified information appeared in the U.S. press. This spearheaded the uniformity in classification between the UK and the United States.

**United States**

**Introduction**

A security clearance is an official determination that an individual may access information [classified](http://en.wikipedia.org/wiki/Classified_information_in_the_United_States) by the United States Government. Security clearances are hierarchical; each level grants the holder access to information in that level and the levels below it. The clearance process requires a background investigation and the signing of a nondisclosure agreement. Access to any particular piece of information requires "need-to-know." In some cases, this requirement is only nominal, as some classified information is widely published on secure networks. In other cases, there is a formal need-to-know determination. In addition to such a determination, [Special Access Programs](http://en.wikipedia.org/wiki/Special_Access_Program) and [Sensitive Compartmented Information](http://en.wikipedia.org/wiki/Sensitive_Compartmented_Information) may require additional investigation and adjudication of the prospective clearance holder.

**Authority**

The authority for classifying information and granting security clearances to access that information is found in executive orders (EOs) and Federal law. National Security Information (NSI) is classified under [EO 13526](http://edocket.access.gpo.gov/2010/pdf/E9-31418.pdf). Information may be classified under this Order if a classification authority determines its unauthorized release could cause damage to the national defense or foreign relations of the United States. Information concerning nuclear weapons and fissile material may be classified under the [Atomic Energy Act of 1954](http://en.wikipedia.org/wiki/Atomic_Energy_Act_of_1954) (AEA). These clearances are only granted by the Department of Energy. The clearance process for access to NSI or AEA information is substantially aligned. Under [EO 12968](http://www.gpo.gov/fdsys/pkg/FR-1995-08-07/pdf/95-19654.pdf), the investigative and adjudicative guidelines for NSI and AEA clearances are identical. This enables reciprocity between NSI and AEA clearances, although some exceptions exist.

Executive Order 12968's standards are binding on all government agencies that handle classified information, but it allows certain agency heads to establish Special Access Programs (SAPs) with additional, but not duplicative, investigative and adjudicative requirements. The [Intelligence Community's](http://en.wikipedia.org/wiki/United_States_Intelligence_Community) Sensitive Compartmented Information (SCI) control systems are a family of SAPs, and SCI eligibility must be granted prior to accessing any particular control system or compartment (which may require additional investigation or adjudication). SCI eligibility policy is described in [Intelligence Community Directive 704](http://www.odni.gov/files/documents/ICD/ICD_704.pdf) and its implementing [policy guidance](http://www.odni.gov/index.php/intelligence-community/ic-policies-reports/intelligence-community-policy-guidance?highlight=YToyOntpOjA7czo1OiJpY3BncyI7aToxO3M6NDoiaWNwZyI7fQ==). Any additional clearance measures used by SAPs must be approved by the [Office of Management and Budget](http://en.wikipedia.org/wiki/Office_of_Management_and_Budget), which has generally limited such measures to polygraphs, exclusion of persons with non-US immediate family members, requiring more frequent reinvestigations, and requiring annual updates to security questionnaires.

**Hierarchy**

Main article: [Classified information in the United States](http://en.wikipedia.org/wiki/Classified_information_in_the_United_States)

A security clearance is granted to an individual and generally recognizes a maximum *level* of clearance. Exceptions include levels above compartmentalized access or when an individual is cleared for a certain *type* of data. The [President of the United States](http://en.wikipedia.org/wiki/President_of_the_United_States) may be given access to any government or military information that he requests if there is a proper "need to know", even if he would not otherwise be able to normally obtain a security clearance were he not the President. Having obtained a certain level security clearance does not mean that one automatically has access to or is given access to information cleared for that clearance level in the absence of a demonstrated "need to know". The "need-to-know" determination is made by a 'disclosure officer,' who may work in the office of origin of the information. The specified "need to know" must be germane to the prospective user's mission, or of necessity for the integrity of a specified security apparatus.

**Controlled Unclassified**

"Controlled Unclassified" does not represent a clearance designation, but rather a clearance level at which information distribution is controlled. Controlled Unclassified designates information that may be illegal to distribute. This information is available when needed by government employees, such as Department of Defense (DoD) employees, but the designation signifies that the information should not be redistributed to users not designated to use it on an operational basis. For example, the organization and processes of an information-technology system may be designated Controlled Unclassified to users for whom the operational details of the system are non-critical.

**Public Trust Position**

Despite common misconception, this designation is not a security clearance, and is not the same as the confidential designation. Certain positions which require access to sensitive information, but not information which is classified, must obtain this designation through a background check. Public Trust Positions can either be moderate-risk or high-risk.

**Confidential**

This is hierarchically the first security clearance to get, typically requiring a few weeks to a few months of investigation. A Confidential clearance requires a [NACLC](http://en.wikipedia.org/wiki/National_Agency_Check_with_Local_Agency_Check_and_Credit_Check) investigation which dates back 7 years on the subject's record and must be renewed (with another investigation) every 15 years.

**Secret**

A Secret clearance, also known as Collateral Secret or Ordinary Secret, requires a few months to a year to investigate, depending on the individual's background. Some instances wherein individuals would take longer than normal to be investigated are many past residences, having residences in foreign countries, having relatives outside the United States, or significant ties with non-US citizens. Unpaid bills as well as criminal charges will more than likely disqualify an applicant for approval. However, a bankruptcy will be evaluated on a case-by-case basis and is not an automatic disqualifier. Poor financial history is the number-one cause of rejection, and foreign activities and criminal record are also common causes for disqualification. A Secret clearance requires a NACLC, and a Credit investigation; it must also be re-investigated every 10 years.[[15]](http://en.wikipedia.org/wiki/Security_clearance#cite_note-renewal-15#cite_note-renewal-15) Investigative requirements for DoD clearances, which apply to most civilian contractor situations, are contained in the Personnel Security Program issuance known as [DoD Regulation 5200.2-R](http://eisen-shapiro.com/WebMaterials/52002r.pdf), at part C3.4.2

**Top Secret**

Top Secret is a more stringent clearance. A Top Secret, or "TS", clearance, is often given as the result of a [Single Scope Background Investigation](http://en.wikipedia.org/wiki/Single_Scope_Background_Investigation), or SSBI. Top Secret clearances, in general, afford one access to data that affects [national security](http://en.wikipedia.org/wiki/National_security), [counterterrorism](http://en.wikipedia.org/wiki/Counterterrorism)/[counterintelligence](http://en.wikipedia.org/wiki/Counterintelligence), or other highly sensitive data. There are far fewer individuals with TS clearances than Secret clearances. A TS clearance can take as few as 3 to 6 months to obtain, but often it takes 6 to 18 months. The SSBI must be reinvestigated every 5 years. In order to receive TS clearance, all candidates must pass an oral interview.

**Compartmented**

As with TS clearances, [Sensitive Compartmented Information](http://en.wikipedia.org/wiki/Sensitive_Compartmented_Information) (SCI) clearances are assigned only after one has been through the rigors of a [Single Scope Background Investigation](http://en.wikipedia.org/wiki/Single_Scope_Background_Investigation) and a special adjudication process for evaluating the investigation. SCI access, however, is assigned only in "[compartments](http://en.wikipedia.org/wiki/Compartmentalization_(intelligence))". These compartments are necessarily separated from each other with respect to organization, so that an individual with access to one compartment will not necessarily have access to another. Each compartment may include its own additional special requirements and clearance process. An individual may be granted access to, or [read into](http://en.wikipedia.org/wiki/Read_into), a compartment for any period of time.

Top secret clearance might be required to access:

* Communications intelligence, a subset of [SIGINT](http://en.wikipedia.org/wiki/SIGINT)
* Design or stockpile information about [nuclear weapons](http://en.wikipedia.org/wiki/Nuclear_weapons)
* Nuclear targeting

Such compartmentalized clearances may be expressed as "John has a TS/SCI", whereby all clearance descriptors are spelled out verbally. For example, the U.S. [National Security Agency](http://en.wikipedia.org/wiki/National_Security_Agency) once used specialized terms such as "Umbra", This classification is reported to be a compartment within the "Special Intelligence" compartment of SCI. The various NSA compartments have been simplified; all but the most sensitive compartments are marked "CCO", meaning "handle through [COMINT](http://en.wikipedia.org/wiki/COMINT) channels only".

The U.S. Department of Defense establishes, separately from intelligence compartments, **special access programs** (SAP) when the vulnerability of specific information is considered exceptional and the normal criteria for determining eligibility for access applicable to information classified at the same level are not deemed sufficient to protect the information from unauthorized disclosure. The number of people cleared for access to such programs is typically kept low. Information about [stealth technology](http://en.wikipedia.org/wiki/Stealth_technology), for example, often requires such access.

Area-specific clearances include:

* [L clearance](http://en.wikipedia.org/wiki/L_clearance) (Department of Energy)
* [Q clearance](http://en.wikipedia.org/wiki/Q_clearance) (Department of Energy)
* [Yankee White](http://en.wikipedia.org/wiki/Yankee_White) (working with the President and Vice President)

**Jobs that require a clearance**

Anyone with access to classified data requires a clearance at or higher than the level at which the data is classified. For this reason, security clearances are required for a wide range of jobs, from senior management to [janitorial](http://en.wikipedia.org/wiki/Janitor). According to a 2010 [*Washington Post*](http://en.wikipedia.org/wiki/Washington_Post) article, 854,000 Americans had top-secret clearances; almost one-third of them worked for private companies, rather than for the U.S. government.

Jobs that require a security clearance can be found either as positions working directly for the federal government or as authorized federal contractors. Over time, more clearance jobs are being outsourced to contractors. Due to an overall shortage in security-cleared candidates and a long time frame to obtain the credentials for an uncleared worker, those with clearance are often paid more than their non-cleared equivalent counterparts. According to one 2010 estimate, "people with security clearances are in the top 10 percent of wage earners in the country".

**Requirements for a clearance**

The [vetting](http://en.wikipedia.org/wiki/Vetting) process for a security clearance is usually undertaken only when someone is hired or transferred into a position that requires access to classified information. The employee is typically [fingerprinted](http://en.wikipedia.org/wiki/Fingerprint) and asked to provide information about themselves. This becomes a starting point for an investigation into the candidate's suitability. The process has been streamlined and now requires the person who needs clearance to input the information online using [E-qip](http://en.wikipedia.org/wiki/E-qip); five days are allowed for data input. Having the older paper form can be helpful for collecting and organizing the information in advance. The information on an investigation and its status is stored in either [JPAS](http://en.wikipedia.org/wiki/E-qip) or [Scattered Castles](http://en.wikipedia.org/wiki/E-qip).

Investigative work is usually at least one of the following types:

* [National Agency Check with Local Agency Check and Credit Check](http://en.wikipedia.org/wiki/National_Agency_Check_with_Local_Agency_Check_and_Credit_Check) (NACLC). An NACLC is required for a Secret, L, and CONFIDENTIAL access. (*See:* [Background check](http://en.wikipedia.org/wiki/Background_check))
* [Single Scope Background Investigation](http://en.wikipedia.org/wiki/Single_Scope_Background_Investigation) (SSBI). An SSBI is required for Top Secret, Q, and SCI access, and involves agents contacting employers, coworkers and other individuals. Standard elements include checks of employment; education; organization affiliations; local agencies; where the subject has lived, worked, or gone to school; and interviews with persons who know the individual. The investigation may include an NACLC on the candidate’s spouse or cohabitant and any immediate family members who are U.S. citizens other than by birth or who are not U.S. citizens.
* [Polygraph](http://en.wikipedia.org/wiki/Polygraph). Some agencies may require polygraph examinations. The most common examinations are Counter Intelligence (CI) and Full-Scope (Lifestyle) polygraphs. While a positive SSBI is sufficient for access to SCI-level information, polygraphs are routinely administered for "staff-like" access to particular agencies.

If issues of concern surface during any phase of security processing, coverage is expanded to resolve those issues. At lower levels, *interim* clearances may be issued to individuals who are presently under investigation, but who have passed some preliminary, automatic process. Such automatic processes include things such as [credit checks](http://en.wikipedia.org/wiki/Credit_check), [felony](http://en.wikipedia.org/wiki/Felony) checks, and so on. An interim clearance may be denied (although the final clearance may still be granted) for having a large amount of debt, having a foreign spouse, for having admitted to seeing a doctor for a [mental health](http://en.wikipedia.org/wiki/Mental_health) condition, or for having admitted to other items of security concern (such as a criminal record or a history of drug use.)

Investigations conducted by one federal agency are no longer supposed to be duplicated by another federal agency when those investigations are current within 5 years and meet the scope and standards for the level of clearance required. The high-level clearance process can be lengthy, sometimes taking a year or more. In recent years, there has been an increased backlog of cases which has been attributed to the economic climate. The long time needed for new appointees to be cleared has been cited as hindering U.S. [presidential transitions](http://en.wikipedia.org/wiki/Presidential_transition).

**Security briefings**

In the U.S., once the clearance is granted, the candidate is briefed on "the proper safeguarding of classified information and on the criminal, civil, and administrative sanctions that may be imposed on an individual who fails to protect classified information from unauthorized disclosure." He or she is also required to sign an approved [non-disclosure agreement](http://en.wikipedia.org/wiki/Non-disclosure_agreement) (e.g., [form SF-312](http://en.wikipedia.org/wiki/Form_SF-312)). High-level clearances are reviewed periodically and any "adverse information" reports received at any time can trigger a review. When a cleared person leaves their job, they are often "debriefed"—reminded of their ongoing obligations to protect the information they were allowed to see. According to NISPOM Chapter 3, newly cleared employees are required to receive an initial security briefing before having access to classified information. This training helps them understand the threat, risks to classified information, how to protect the classified information, security procedures and duties as they apply to their job. This training is followed up by refresher training that reinforces the initial security briefing.

**Dual citizenship**

[Dual citizenship](http://en.wikipedia.org/wiki/Dual_citizenship) is associated with two categories of security concerns: foreign influence and foreign preference. Dual citizenship in itself is not the major problem in obtaining or retaining security clearance in the United States. If a security clearance applicant's dual citizenship is "based solely on parents' citizenship or birth in a foreign country", that can be a mitigating condition. However, *exercising* (taking advantage of the entitlements of) a non-U.S. citizenship can cause problems. For example, possession and/or use of a foreign [passport](http://en.wikipedia.org/wiki/Passport) is a condition disqualifying from security clearance and "is not mitigated by reasons of personal convenience, safety, requirements of foreign law, or the identity of the foreign country" as is explicitly clarified in a Department of Defense policy memorandum which defines a guideline requiring that "any clearance be denied or revoked unless the applicant surrenders the foreign passport or obtains official permission for its use from the appropriate agency of the United States Government". This guideline has been followed in [administrative rulings](http://www.dod.mil/dodgc/doha/industrial/) by the [Department of Defense](http://en.wikipedia.org/wiki/United_States_Department_of_Defense) (DoD) [Defense Office of Hearings and Appeals](http://www.dod.mil/dodgc/doha/) (DOHA) office of [Industrial Security Clearance Review](http://www.dod.mil/dodgc/doha/isp.html) (ISCR), which decides cases involving security clearances for Contractor personnel doing classified work for all DoD components. In one such case, an administrative judge ruled that it is not clearly consistent with U.S. national interest to grant a request for a security clearance to an applicant who was a dual national of the United States and Ireland.

**Individuals who have had security clearances revoked**

In the post [World War II](http://en.wikipedia.org/wiki/World_War_II) era there have been several highly publicized, and often controversial, cases of officials or scientists having their security clearances revoked, including:

* [Sandy Berger](http://en.wikipedia.org/wiki/Sandy_Berger)
* [John M. Deutch](http://en.wikipedia.org/wiki/John_M._Deutch)
* [Abdel-Moniem El-Ganayni](http://en.wikipedia.org/wiki/Abdel-Moniem_El-Ganayni)
* [Wen Ho Lee](http://en.wikipedia.org/wiki/Wen_Ho_Lee)
* [Robert Oppenheimer](http://en.wikipedia.org/wiki/Robert_Oppenheimer)
* [Alan Turing](http://en.wikipedia.org/wiki/Alan_Turing) [(UK)](http://en.wikipedia.org/wiki/United_Kingdom)
* [Qian Xuesen](http://en.wikipedia.org/wiki/Qian_Xuesen)
* [Edward Snowden](http://en.wikipedia.org/wiki/Edward_Snowden)

**United Nations**

The UN has a Security Clearance (SC) procedure and document for [United Nations](http://en.wikipedia.org/wiki/United_Nations) staff travelling to areas designated as [security phase](http://en.wikipedia.org/w/index.php?title=Security_phase&action=edit&redlink=1) areas, with numbers ranging from one to five ("no-phase" areas are calm countries where no SC is required).

[United Nations](http://en.wikipedia.org/wiki/United_Nations) staff can apply for SC online, at the website of the [Department for Safety and Security](http://en.wikipedia.org/wiki/Department_for_Safety_and_Security).

**See also**

* [Background check](http://en.wikipedia.org/wiki/Background_check)
* [Compartmentalization (intelligence)](http://en.wikipedia.org/wiki/Compartmentalization_(intelligence))
* [List of U.S. security clearance terms](http://en.wikipedia.org/wiki/List_of_U.S._security_clearance_terms)
* [Security Advisory Opinion](http://en.wikipedia.org/wiki/Security_Advisory_Opinion)

**External links**

**Canada**

* [Standard on Security Screening](http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=28115)

**UK**

* [UK MOD's Defence Vetting Agency](http://www.mod.uk/DefenceInternet/AboutDefence/WhatWeDo/SecurityandIntelligence/DVA/)

**US**

* [(DoD) Factors Used for Determining Security Clearance Approval/Disapproval](http://usmilitary.about.com/od/theorderlyroom/l/blsecmenu.htm)
* [Defense Office of Hearings and Appeals decisions](http://www.dod.mil/dodgc/doha/industrial/)
* [Security Clearance FAQs](http://www.clearancejobs.com/security_clearance_faq.pdf)
* [How to get clearance](http://www.jobsforuscitizens.com/how-to-get-us-security-clearance)
* [DoD Intelligence & Security Documents, directives and Instructions](http://www.fas.org/irp/doddir/dod/index.html)
* [DoD Security Clearances and Contracts Guidebook-What You Need to Know About Your Need to Know](http://books.google.com/books?id=EjVHMRx-zakC&pg=PA290&lpg=PA290&dq=clearance+jobs,+bennett&source=bl&ots=Z1noDeJH1B&sig=ow_1E2f-j02USSuK1TU3bwIVx4Q&hl=en&ei=UYhXToLZH8y2tgeXrs2dDA&sa=X&oi=book_result&ct=result&resnum=7&sqi=2&ved=0CHIQ6AEwBg#v=onepage&q&f=false)
* [Federal Suitability Security Clearance Chart](http://fedcas.com/wp-content/uploads/2012/05/Federal-Suitability-Security-Clearance-Chart.pdf)
* [Defense Office of Hearings and Appeals (DOHA) Experiencing Immense Backlog of Cases, Highlighting Need for Thorough and Effective Preparation of Clearance Applications](http://www.natlawreview.com/article/defense-office-hearings-and-appeals-doha-experiencing-immense-backlog-cases-highligh)

**UN**

* [United Nations Department of Safety and Security](http://dss.un.org)

**Geneva Centre for the Democratic Control of Armed Forces**

* [Vetting and the Security Sector](http://www.dcaf.ch/Publications/Vetting-and-the-Security-Sector), published by [DCAF](http://en.wikipedia.org/wiki/Geneva_Centre_for_the_Democratic_Control_of_Armed_Forces)

"<http://en.wikipedia.org/w/index.php?title=Security_clearance&oldid=632977777>"

[Categories](http://en.wikipedia.org/wiki/Help:Category):

* [Espionage](http://en.wikipedia.org/wiki/Category:Espionage)
* [National security](http://en.wikipedia.org/wiki/Category:National_security)
* [United States government secrecy](http://en.wikipedia.org/wiki/Category:United_States_government_secrecy)
* [United Nations legislation](http://en.wikipedia.org/wiki/Category:United_Nations_legislation)

This page was last modified on 8 November 2014 at 17:23.