**National Security and Access Clearances**

Security clearances have always been shrouded in ambiguity. Most people have no clear understanding for what is granted to what purpose. Since I held most of these at one time or other, I will describe their functions and purpose to dispel its mystery.

Security clearance is a status granted individuals, typically to members of the military and employees of governments and their contractors, allowing them access to classified information. The term ‘security clearance’ is also used in private organizations that have a formal process to examin employees for access to sensitive information. A clearance by itself is normally not sufficient to gain access; the organization must determine that the cleared individual has a ‘need to know’ for the information. No one is supposed to be granted access to classified information solely because of rank, position, or a security clearance.

Classified information is sensitive 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 act of assigning the level of sensitivity to data is termed data classification.

The type of clearances issued is following: Unclassified, Restricted, Noforn, Confidential, Secret, Top Secret, and Ultra Secret or SCI.

Government organizations, especially those related to defence and intelligence, often deal with information considered very sensitive. The ‘Need to Know’ is one principle which can be used to attempt to secure such information.

The principle is such that, even if someone has all the necessary official approvals (such as a security clearance) to access certain information they should not be given access to such information unless they have a need to know: that is, access to the specific information necessary for the conduct of one's official duties. In essence, the principle aims to discourage ‘browsing’ of sensitive material, thereby limiting access to the smallest possible number of people.

The discretionary access control mechanisms of some operating systems can be used to enforce need to know. In this case, the owner of a file determines whether another person should have access. Need to know is often concurrently applied with mandatory access control schemes, in which the lack of an official approval (such as a clearance) may absolutely prohibit a person from accessing the information. This is because need to know can be a subjective assessment.

It has been alleged that need to know (like other security measures) can be misused by some personnel who wish to refuse others access to information they hold, in an attempt to increase their personal power, or to prevent unwelcome review of their work.

As with most security mechanisms, the aim is to make it difficult for unauthorised access to occur, without inconveniencing legitimate access. In some situations, such as intelligence analysis or research, the need to know principle can be problematic, because it is difficult to determine that a person has a need to know until the information has been accessed and assessed. Sensitive information is information or knowledge that might result in loss of an advantage or level of security if revealed (disclosed) to others who might have low or unknown trustability and/or indeterminable or hostile intentions.

Loss, misuse, modification or unauthorized access to sensitive information can adversely affect the privacy of an individual, trade secrets of a business or even the security, internal and foreign affairs of a nation depending on the level of sensitivity and nature of the information.

**Hierarchy**

A security clearance is generally granted to a particular level of clearance. The exception to this is levels above compartmentalized access, when an individual is given access to a particular type of data.

**Unclassified**

Unlcassified is all informaiton and knowledge free from restrictions and open to public for access and viewing. Technically, it is not a classification level, but is used for government documents that do not have a classification listed. Such documents can be viewed by those without security clearance.

**Restricted**

Restricted access is material the would cause ‘undesirable’ effects if publicly available. Some countries do not have such a classification.

**Noforn**

Noforn or ‘No Foreign’ is the classification of information and knowledge restrictions to individuals from foreign countries. Access is granted to only U.S. citizens.

**Confidential**

Confidential is the simplest security clearance. This level typically requires a few weeks to a few months of investigation. A Confidential clearance requires a background check required in the United States for granting of security clearances. This is generally performed as National Agency Check through Local Agency Check and Credit Check (NACLC) as type of background check required in United States for granting of security clearances. The NACLC investigation must be renewed every 15 years. Such material would cause ‘damage’ or be ‘prejudicial’ to national security if publicly available.

The background check is a method of acquiring information on an individual through third-party services, government organizations and private individuals in the hopes of making a determination on the future actions of an individual based on past actions. Information gathered in a background check can be abused and used to commit identity theft. The right to request background checks is enforced by the Patriot Act, as well as other Federal laws which surround the right of organizations to pursue information to make financial determinations before submitting to contracts.

**Secret**

A Secret clearance, also known as ‘Ordinary Secret’, requires a few months to a year to fully investigate depending on the individual's activities. Some instances where individuals would take longer than normal to be investigated are many past residences, having residences in foreign countries, or have relatives outside the United States. Bankruptcy and unpaid bills as well as criminal charges will also increase the time of both the investigation and approval. A Secret clearance requires a NAC/LAC/Credit investigation and must be reinvestigated every 10 years. Such material would cause ‘serious damage’ to national security if publicly available.

**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, or SSBI. Top Secret clearances generally provide one access to data that affects national security, counterterrorism and counterintelligence, or other highly sensitive data. There are far fewer individuals with TS clearances than Secret clearances. A TS clearance can take as little as 3-6 months to obtain, but more often takes 6-18 months, while sometimes taking up to 3 years to obtain. The SSBI investigation must be reinvestigated every 5 years. It is the highest level of classification of material. Such material would cause ‘exceptionally grave damage’ to national security if publicly available.

A Single Scope Background Investigation (SSBI) is a type of United States security clearance investigation required for Top Secret, Q, and SCI access, and involves agents contacting employers, coworkers and other individuals. Standard elements include background checks involving 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 a 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.

**Compartments of Top Secret**

* *ATOMAL:* Atomic Energy Experimental Nuclear Weapons Test Data
* *COMSEC:* Communications Security Signal Intelligence
* *COSMIC:* Cosmic Intelligence UFO Activities & Action Plan
* *CRYPTO:* Cryptographic Facility Access Handling
* *EAP:* Emergency Action Procedures
* *ESI:* Extremely Sensitive Information
* *LeeMah:* Classified Military Networks and Signals
* *NATO:* North Atlantic Treaty Organization
* *SIOP:* Single Integrated Operations Plan
* *WINTEL:* Warning! Intelligence Sources or Methods Involved

**Sensitive Compartmented Information (SCI)**

As with TS clearances, Sensitive Compartmented Information (SCI) clearances are assigned only after one has been through the rigors of a Single Scope Background Investigation. SCI access, however, is assigned only in ‘compartments.’ These compartments are necessarily separated from each other organizationally, therefore, an individual with access to one compartment will not necessarily have access to another. Each compartment may include its own additional clearance process.

**Compartments of SCI**

* *Crypto*: Cryptography
* *TK*: Satellite intelligence
* *SI*: Special Intelligence (primarily intelligence organizations)
* *Q*: Department of Energy Nuclear Weapons

Such compartmentalized clearances may be expressed as ‘John has a TS/SCI TK/Q clearance’, where all clearance descriptors are spelled out verbally. Certain government departments may also establish special access programs (SAP) when vulnerability of specific information is 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, for example, often requires such access.

**Clearance Requirements**

The examination and evaluation 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 and asked to fill out a detailed life history form, including all foreign travel, which becomes a starting point for an investigation into the candidate's suitability. This process can include several types of investigations, depending on the level of clearance required:

* National Agency Check with Local Agency Check and Credit Check (NACLC). An NACLC is required for a Secret, Limited, and Confidential access.
* 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. 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 whom have passed some preliminary, automatic process. Such automatic processes include things such as credit checks, 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 or having admitted to seeing a doctor for a mental health condition.

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. The long time needed for new appointees to be cleared has been cited as hindering U.S.

The amount of information included on a background check depends to a large degree on the sensitivity of the reason for which it is conducted e.g., somebody seeking employment at a minimum wage job (such as a janitor cleaning a secure facility) would be subject to far fewer background check requirements than somebody applying to work for the FBI.

**Background Checks**

* Criminal and incarceration records.
* Litigation records. Employers may want to identify potential employees who routinely file discrimination lawsuits. It has also been alleged that in the U.S., employers that do work for the government do not like to hire whistleblowers who have a history of filing falseclaim suits.
* Driving and vehicle records. Employers in the transportation sector seek drivers with clean driving records--i.e., those without a history of accidents or traffic tickets.
* Drug tests are used for a variety of reasons--corporate ethics, measuring potential employee performance, and keeping workers' compensation premiums down.
* Education records. These are used primarily to see if the potential employee had in fact received a college degree. There are reports of SAT scores being requested by employers as well.
* Employment records. These usually range from simple verbal confirmations of past employment and timeframe to deeper, such as discussions about performance, activities and accomplishments, and relations with others.
* Financial information: Individuals with poor credit scores, liens, civil judgments, or those who have filed for bankruptcy may be at an additional risk of stealing from the company.
* Licensing records. A government authority that has some oversight over professional conduct of its licensees will also maintain records regarding the licensee, such as personal information, education, complaints, investigations, and disciplinary actions.
* Military records. Although not as common today as it was in the past fifty years, employers frequently requested the specifics of one's military discharge.
* Social Security Number (or equivalent outside the US). A fraudulent SSN may be indicative of identity theft, insufficient citizenship, or concealment of a ‘past life’.
* Polygraph test. Also known as a psychophysiological detection of deception (PDD) examination.
* Other interpersonal interviews. Employers will usually wish to speak with potential employees' references to gauge employability. More intensive background checks can involve interviews with anybody that knew or previously knew the applicant--such as teachers, friends, coworkers, and family members.

### 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 (e.g. 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.

**Sensitive Information**

Classified information is ‘Sensitive Information’ to which access is restricted by law or regulation to particular classes of people. The act of assigning the level of sensitivity to data is called data classification. The term classified information generally refers to information that is subject to special security classification regulations imposed by many national governments. The term Unclassified as used in the table below refers to information that is not subject to security classification regulations.

In the intelligence community the sensitivity indicator specifies the level of secrecy of a project, document or piece of information by its relevancy to national security. Only those with appropriate security clearances can access information of certain sensitivity and might face additional special access restrictions. The indicator can also be the name of a classified project such as ‘Project Blue Book’ or ‘ULTRA’, to further restricting access to or handling of information.

Ultra (sometimes capitalized ULTRA) was the name used by the British for intelligence resulting from decryption of German communications in World War II. The term eventually became the standard designation in both Britain and the United States for all intelligence from high-level cryptanalytic sources. The name arose because the code-breaking success was considered more important than the highest security classification available at the time (Most Secret) and regarded as being Ultra secret.

**Security Compromise**

In the security field, the term compromise refers to a state of deviance from an optimal state of absolute security—either in reference to a problem with security protocols without reference to any damages, or to acts which are considered damages as follows:

* The known or suspected exposure of clandestine personnel, installations, or other assets or of classified information or material, to an unauthorized person.
* The disclosure of cryptographic information to unauthorized persons.
* The recovery of plaintext of encrypted messages by unauthorized persons through cryptanalysis methods.
* The disclosure of information or data to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.

**Encryption**

In cryptography, encryption is the process of obscuring information to make it unreadable without special knowledge. While encryption has been used to protect communications for centuries, only organizations and individuals with an extraordinary need for secrecy had made use of it. In the mid-1970s, strong encryption emerged from the sole preserve of secretive government agencies into the public domain, and is now employed in protecting widely-used systems, such as Internet e-commerce, mobile telephone networks and bank automatic teller machines.

Encryption can be used to ensure secrecy, but other techniques are still needed to make communications secure, particularly to verify the integrity and authenticity of a message; for example, a message authentication code (MAC) or digital signatures. Another consideration is protection against traffic analysis.

Encryption or software code obfuscation is also used in software copy protection against reverse engineering, unauthorized application analysis, cracks and software piracy used in different encryption or obfuscating software.

**Ciphers**

A cipher is an algorithm for performing **encryption** (and the reverse, decryption) — a series of well-defined steps that can be followed as a procedure. An alternative term is encipherment.

The original information is known as plaintext, and the encrypted form as ciphertext. The ciphertext message contains all the information of the plaintext message, but is not in a format readable by a human or computer without the proper mechanism to decrypt it; it should resemble random gibberish to those not intended to read it.

The operation of a cipher usually depends on a piece of auxiliary information, called a key or, in traditional NSA parlance, a cryptovariable. The encrypting procedure is varied depending on the key, which changes the detailed operation of the algorithm. A key must be selected before using a cipher to encrypt a message. Without knowledge of the key, it should be difficult, if not impossible, to decrypt the resulting ciphertext into readable plaintext.

‘Cipher’ is alternatively spelled ‘cypher’; similarly ‘ciphertext’ and ‘cyphertext’, and so forth is the word descends from the Arabic word for zero (which remaines in use for 0, the crucial innovation in positional Arabic versus Roman numerals) but soon was used for any decimal digit, even any number.

**Ciphers versus codes**

In non-technical usage, a ‘(secret) code’ is the same thing as a cipher. Within technical discussions, however, they are distinguished into two concepts. Codes work at the level of meaning — that is, words or phrases are converted into something else and this chunking generally shortens the message. Ciphers, on the other hand, work at a lower level: the level of individual letters, small groups of letters, or, in modern schemes, individual bits. Some systems used both codes and ciphers in one system, using superencipherment to increase the security.

Historically, cryptography was split into a dichotomy of codes and ciphers, and coding had its own terminology, analogous to that for ciphers: ‘encoding, codetext, decoding’ and so on. However, codes have a variety of drawbacks, including susceptibility to cryptanalysis and the difficulty of managing a cumbersome codebook. Because of this, codes have fallen into disuse in modern cryptography, and ciphers are the dominant technique.

**Types of cipher**

There are a variety of different types of encryption. Algorithms used earlier in the history of cryptography are substantially different from modern methods, and modern ciphers can be classified according to how they operate and whether they use one or more keys.

Historical pen and paper ciphers used in the past are sometimes known as classical ciphers. They include simple substitution ciphers and transposition ciphers. For example GOOD DOG can be encrypted as PLLX XLP where L substitutes for O throughout the message. Transposition of the letters GOOD DOC can result in DDOCOGO. These simple ciphers are easy to crack, even without plaintext-ciphertext pairs.

Simple ciphers were replaced by polyalphabetic substitution ciphers which changed the substitution alphabet for every letter. With even a small amount of known plaintext, polyalphabetic substitution ciphers and letter transposition ciphers designed for pen and paper encryption are easy to crack.

During the early twentieth century, electro-mechanical machines were invented to do encryption and decryption using a combination of transposition, polyalphabetic substitution, and ‘additive’ substitution. In rotor machines, several rotor disks provided polyalphabetic substitution, while plug boards provided transposition. Keys were easily changed by changing the rotor disks and the plugboard wires. Although these encryption methods were more complex than previous schemes and required machines to encrypt and decrypt, other machines such as the British Bombe were invented to crack these encryption methods.

Modern encryption methods can be divided into symmetric key algorithms (Private-key cryptography) and asymmetric key algorithms (Public-key cryptography). In a symmetric key algorithm (e.g., DES and AES), the sender and receiver must have a shared key set up in advance and kept secret from all other parties; the sender uses this key for encryption, and the receiver uses the same key for decryption. In an asymmetric key algorithm (e.g., RSA), there are two separate keys: a public key is published and enables any sender to perform encryption, while a private key is kept secret by the receiver and enables only him to perform decryption.

**Key size and vulnerability**

In a pure mathematical attack (i.e., lacking any other information to help break a cypher), three factors above all, count:

* Mathematical advances, that allow new attacks or weaknesses to be discovered and exploited.
* Computational power available, i.e. the computer power which can be brought to bear on the problem.
* Key size, i.e., the size of key used to encrypt a message. As the key size increases, so does the complexity of brute search to the point where it becomes infeasible to crack encryption directly.

Since the desired effect is computational difficulty, in theory one would choose an algorithm and desired difficulty level, thus decide the key length accordingly.

**Methods of Compromise**

A typical security compromise and challenge was the German Naval Enigma. Even before the war, it had been a challenge to the Poles; only a portion of Naval Enigma had been read at B.S.-4 (the Cipher Bureau's German section) due to limited bureau personnel and resources and because knowledge of army and air force traffic had been deemed more important to Poland's defense.

One mode of attack on the Enigma relied on the fact that the reflector (a patented feature of the Enigma machines) guaranteed that no letter could be enciphered as itself, so an ‘A’ could not be sent as an A. Another technique counted on common German phrases, such as ‘Heil Hitler’ or ‘please respond,’ which were likely to occur in a given plaintext; a successful guess as to a plaintext was known at Bletchley as a crib (cryptanalysis.) With a probable plaintext fragment and the knowledge that no letter could be enciphered as itself, a corresponding ciphertext fragment could often be identified. This provided a clue to message keys.

Bletchley Park, also known as Station X, is an estate located in the town of Bletchley, now part of Milton Keynes, England. During World War II, Bletchley Park was the location of the United Kingdom's main codebreaking establishment. Codes and ciphers of several Axis countries were deciphered there, most famously the German Enigma. The high-level intelligence produced by Bletchley Park, codenamed Ultra, is frequently credited with aiding the Allied war effort and shortening the war, although Ultra's effect on the actual outcome of WWII is debated.

On some occasions, German cipher clerks helped Allied cryptanalysts. In one instance, a clerk was asked to send a test message, and hit the ‘T’ key repeatedly and transmitted the resulting letters. A British analyst received from an intercept station a long message containing not a single ‘T’ and immediately realised what had happened. In other cases, as they had before the war, Enigma operators would constantly use the same settings for their message keys, often their own initials or those of a girlfriend (one clerk had a girlfriend named Cillie, and would continuously use CIL as the rotor setup. Bletchley Park named such hints ‘cillies’). Analysts were set to finding such messages in the sea of daily intercepts, which filtered out enough possibilities to allow Bletchley to use other original Polish techniques as well to find the initial daily keys. Other German operators used ‘form letters’ for daily reports, notably weather reports, so the same crib might be used every day.

Had the Germans ever replaced every rotor at the same time, the British might not have been able to break back into the system. And had German operating practices been more secure, things would have been much more difficult for the British cryptologists. However, due to the expense and difficulty of getting new rotors to all ships and units, this proved impratical. Instead the Germans every so often added new rotors to the mix, thereby allowing the British to work out the wirings of the newest rotors.

**Code Classifications**

|  |  |  |
| --- | --- | --- |
|  | **RESTRICTED**   * Level 2 (light blue) * requires some protection * requires level 2 security clearance or higher * public disclosure could have undesirable effects or do some harm.   **CONFIDENTIAL**   * Level 3 (blue) * requires protection * requires level 3 security clearance or higher to access * unauthorized disclosure could damage national security e.g. compromise information that indicates the strength of armed forces or disclosure of technical information about weapons, such as performance characteristics, test data, design, and production data.   **SECRET**   * Level 4 (red) * requires substantial protection * requires level 4 security clearance or higher to access * unauthorized disclosure could seriously damage national security. * Wrongful disclosure could lead to a disruption of foreign relations, impair a program or policy directly related to national security, reveal significant military plans or intelligence operations, or compromise significant scientific or technological development relating to national security. * most classified information falls into this category * penalty can be a large fine and/or a 5 year to life imprisonment sentence   **TOP SECRET (TS)**   * Level 5 (orange) * requires the highest degree of protection * requires level 5 security clearance * unauthorized disclosure could severely damage national security * wrongful disclosure could lead to war against a nation or its allies, disrupt vital relations, compromise vital defense plans or cryptologic and communications intelligence systems, reveal sensitive intelligence operations, or could jeopardize a vital advantage in an area of science or technology. * penalty can range from 5 years to life imprisonment or even the death penalty if considered treason.   **ULTRA SECRET or SCI**   * Level 6 (yellow) * requires exceptionally high or special protection * requires level 5 security clearance and special (Q) clearance and or invitation. * unauthorized disclosure could existentially damage national security, international stability or wartime advantage * wrongful disclosure could lead to loss or prolongation of a war, provide enemies with secret weapon technology or inform them of compromised top secret information. * penalty will most likely be capital punishment due to treason. |  |