How the Government Security System Works

Contributed by CRTC Member, Carl Strobel— President, FiberPlus, Inc.

The United States government, along with most governments of the world, has a system to prevent the disclosure of information if that disclosure would harm national security. The system is simple in concept but can be complex in its actual operation.

We're going to look at the two aspects of the system :

I. Security classifications assigned to information
II. Clearances that allow individuals to have access to that information.

Incidentally, the term information is used here in its broadest sense. It can mean the contents of an intelligence report, plans for a special building, access to a piece of advanced equipment, knowledge of sensitive operations, techniques used to gather intelligence and much more.

There are three classifications – **Confidential, Secret and Top Secret** – which are assigned according to the seriousness of the damage to national security that could result from disclosure to the wrong people – actual or potential enemies of the United States.

Confidential is the lowest classification. It is applied to information whose disclosure would *"damage"* national security. It might be applied, for example, to an intelligence agency's internal telephone directory that lists the names and offices of people working there.

Secret means the information would cause *"serious damage."* One example could be plans to conduct a tactical combat operation. The plans would cover only an operation in a limited area for a very limited period of time but premature disclosure could hurt the success of the operation.

Top Secret is the highest level and means the information could cause *"exceptionally grave damage"* or *"loss of life"* if disclosed. An example from history would be the Allies' ability to read many of Germany's encrypted messages during World War II. Knowledge by the Germans that this was happening could have ended the Allies' ability to locate and destroy German submarines as well as achieve a number of other military successes.

Incidentally, the classification of Top Secret was introduced to denote extraordinarily important information when the U.S. and Great Britain were working together reading German coded messages. British Prime Minister Winston Churchill, a serious student of the English language, thought the highest

security classification should have been called “Most Secret”. He thought “Top Secret” sounded like an Americanism. He lost the argument.

There is another category of information, not really a classification, termed “**For Official Use Only**”, usually abbreviated as “**FOUO**”. For example, this could be applied to the printed daily schedule for a military base or a ship – something that is best not given public distribution even though it is not technically classified.

Next we’ll see **how access to classified information is controlled**. This is done by authorizing clearances for individuals to give them that access. The clearances are requested by the individual’s employer and granted only by the government.

The prime rule in the world of classified information is **“Need to Know.”** An individual is only allowed access to that information needed to accomplish his assigned duties. A person therefore is granted a clearance at the Confidential, Secret or Top Secret level depending upon the information he or she will need in the job. A little later we’ll discuss something called **“special access”.**

The requirements to qualify for a clearance naturally get more stringent as you go up the scale. A person might qualify for a Confidential or even a Secret clearance but not a Top Secret clearance.

What is looked at in deciding whether to grant a clearance? First, of course, is **“Need to Know”** – the job for which the individual is being considered must require a clearance. The next hurdle to getting a clearance is **citizenship**. Except in very special circumstances, the U.S. government provides security clearances only to American citizens.

One of the first steps taken to check out an individual is a **search of police records**. A serious crime usually disqualifies the candidate. A minor offense such as a parking ticket or speeding ticket, even more than one, is not a concern. However, a lengthy list of parking tickets could raise a red flag – does this show contempt for rules and authority?

That level of scrutiny along with the recommendation of the employer is usually adequate for a **Confidential or Secret** clearance. But a request for a **Top Secret** clearance requires further investigation in order to make an informed judgment on the reliability of the person. How likely is he or she to give away classified information either accidentally or deliberately? Some people might thoughtlessly talk about their work. Others might be susceptible to blackmail or have desperate financial need. Some might want to impress their friends by telling about the important secrets they know. Others might be willing to trade classified information for money and a luxurious lifestyle. And there are those rare individuals who feel no loyalty to the United States and would help an adversary.

The information to make this judgment is collected through a **Background Investigation**. The candidate for a clearance must fill out an exhaustive form called SF-86 and list residences, schools attended, foreign travel, relatives or friends who are foreign nationals, names of spouses and children, places of employment and the like.

This is used to identify people who can give some evaluation of the candidate's suitability for a clearance. This can include neighbors, employers, coworkers, teachers and people designated by the candidate as personal references. Consequently many of them are interviewed face-to-face by security investigators.

The investigator's questions probe for such factors as the candidate's stability, good judgment, reliability and loyalty to the United States. Interviews typically end with the interviewee being asked if he or she would personally recommend the candidate for a position of trust involving national security. The interviews cover the preceding seven years for a Secret clearance and 10 years for Top Secret.

Answers given during interviews are not always taken at face value. In one instance, a young military recruit from a very rural area in the south was being processed for a Top Secret clearance. Among the people being interviewed was the minister of his church – a very fundamentalist church. The pastor said he couldn't recommend the young man for any position of responsibility or trust – his conduct was reprehensible. Asked what that conduct was, the minister replied that the young man went to movies, even sometimes on Sundays, and went out alone with girls. The recruit got his clearance.

The clearance process also includes a **personal interview** with the individual under consideration.

When all the relevant information has been collected, an experienced security adjudicator analyzes it and recommends either a clearance be granted or be denied. That recommendation is then reviewed, particularly if the initial recommendation was for denial.

Once approved the individual is given a **briefing** in which the security rules for handling classified information are explained and the importance of those rules is stressed.

Some intelligence efforts are so sensitive they must be protected by requiring **"special access".** This would require at the minimum a briefing on the intelligence effort and the reason for its sensitivity and would require a signature attesting that the briefing was conducted. In some cases, additional security investigation must be conducted, such as questioning while a polygraph is operating.

An example of this **"special access"** could be an instance where a source high in an adversarial government was providing U.S. intelligence with detailed information on that government's plans and policies.

As can be seen, the whole intent of the security system is to limit the amount of information provided an individual to that directly needed for performance of duties and to ensure the individual will safeguard that information from disclosure.

We have been talking about security clearances for individuals. However, a company must have formal approval before it can obtain clearances from the government for any of its employees. That approval is called a **Facility Clearance**. It is given the company after a demonstration that it can provide services needed on a classified contract, it is prepared to operate a security program internally and it is not owned or controlled by foreign citizens or government.

The Security Alphabet

Contributed by CRTC Member, Carl Strobel— President, FiberPlus, Inc.

BI -- Background Investigation. An investigation to determine the suitability of an individual to hold a security clearance. It includes a review of public records such as police reports as well as interviews with persons who know or have known the person requesting a clearance.

BI Update – A periodic reinvestigation of a person who holds a security clearance.

Briefing – A presentation given to an individual when a clearance is officially granted. This includes a talk on security rules and the need for security. The individual then signs a written agreement that the rules will be followed.

CyberCom – The U.S. Cyber Command is an organization within the Department of Defense that was established in May, 2010 and is located at Fort Meade. The command's mission is to integrate efforts by the military services to protect their digital networks and infrastructures from disruption or other action by hostile organizations.

Debriefing – A process followed when an individual no longer has the need for a security clearance. The individual is reminded of the obligation to continue to protect information gained during the period of the clearance and signs a written agreement to that effect.

DIA – The Defense Intelligence Agency, an agency within the Department of Defense that produces, analyzes and disseminates intelligence on foreign military capabilities, operations and the like. It is manned by military personnel from the Army, Navy, Air Force and Marine Corps as well as government civilians

DISCO – Defense Industrial Security Clearance Office. Processes requests for clearance for Defense contractors and issues clearances based on an investigation of individuals.

DoD – The Department of Defense.

DNI – Director of National Intelligence. The individual who serves as principal advisor to the President on intelligence matters and directs the national intelligence program. The term can also apply to his organization.

DSS – Defense Security Service. The organization responsible for providing security education and other security services for military personnel, government civilians and contractors working for the Department of Defense. This includes periodic inspections of contractor facilities and reviews of their internal security system.

e-QIP – Electronic Questionnaires for Investigations Processing. e-QIP is a web-based automated system that was designed to facilitate the processing of standard investigative forms used when conducting background investigations. e-QIP allows the user to electronically

enter, update and transmit their personal investigative data over a secure internet connect to a requesting agency. The requesting agency will review and approve the investigative data.

Facility Clearance – Approval by the government for a company to work on classified contracts and request clearances for employees. This is based on a thorough investigation of the company's ownership and its ability to meet security standards.

FOUO – For Official Use Only. Not a clearance but a caveat applied to information that should not be given public distribution.

Industrial Security – That portion of information security concerned with the protection of classified information in the custody of U.S. industry

Intelligence Community – The U.S. Intelligence Community (IC) is comprised of the 17 agencies and organizations within the executive branch of the government that gather intelligence needed to conduct foreign relations and national security activities. The 17 members are Air Force Intelligence, Army Intelligence, Central Intelligence Agency, Coast Guard Intelligence, Defense Intelligence Agency, Department of Energy, Department of Homeland Security, Department of State, Department of the Treasury, Drug Enforcement Administration, Federal Bureau of Investigation, Marine Corps Intelligence, National Geospatial Intelligence Agency, National Reconnaissance Office, National Security Agency, Navy Intelligence and Office of the Director of National Intelligence.

JPAS – The Joint Personnel Adjudication System is a web-based database that unites clearance information on all DoD personnel.

Need to Know – A principle in intelligence work that a person should have access only to that classified information needed for the performance of the person's work.

NISPOM – The National Industrial Security Program Operating Manual is the primary guidance source for all industrial contractors in maintaining security compliance over the management of classified programs.

NSA – The National Security Agency/Central Security Service. The following description of the agency's mission is from the NSA website. "The NSA/CSS core missions are to protect U.S. national security systems and to produce foreign signals intelligence information.
The Information Assurance mission confronts the formidable challenge of preventing foreign adversaries from gaining access to sensitive or classified national security information.
The Signals Intelligence mission collects, processes, and disseminates intelligence information from foreign signals for intelligence and counterintelligence purposes and to support military operations."

OPM – Office of Personnel Management. Conducts the investigations of individuals nominated for clearances.

Personnel (Security) Clearance (PCL) – An administrative determination that an individual is eligible, from a security point of view, for access to classified information of the same or lower category as the level of the personnel clearance being granted.

Poly – Polygraph. Commonly called a lie detector, this device is attached to an individual while that person is questioned about life style, contacts with foreign governments, etc.

SCI – Sensitive Compartmented Information. This is especially sensitive intelligence information that requires special protection. A person granted access to SCI must pass additional security screening.

SF-86 – Standard Form 86. The form filled out by persons applying for a security clearance that asks for such personal information as residences, employers, etc. This information forms the basis for a Background Investigation (See BI).

TS – Top Secret. Highest of the three security classifications.

TS/SCI – Top Secret clearance with access authorized for Sensitive Compartmented Information (see SCI).

For More Information

Intelligence Community
www.intelligence.gov

National Security Agency
www.nsa.gov

Personnel Security Clearances
http://www.dss.mil/psco/ps_faqs.html

Provisional Industrial Security Approval (PISA)
http://www.nsa.gov/business/programs/pisa.shtml

Additional Resources:

http://www.veteranstoday.com/2010/01/25/security-clearances-what-who-when-and-why-get-the-answers/

http://www.clearancejobs.com/security_clearance_faq.pdf