

# Security Clearance Frequently Asked Questions

Questions and answers related to US government-sponsored security clearances in accordance with the National Industrial Security Program (NISP) and compiled by ClearanceJobs.com



## General

### **What is a security clearance?**

A security clearance is a determination by the United States government that a person or company is eligible for access to classified information. There are two types of clearances: Personnel Security Clearances (PCL) and Facility Security Clearance (FCL). Government agencies that issue clearances often refer to clearances as "eligibility for access."

### **What is DISCO?**

The Defense Industrial Security Clearance Office (DISCO) is part of the Defense Security Service (DSS), an agency of the Department of Defense (DoD). DISCO processes and adjudicates Personnel Clearances (PCL) and Facility Clearances (FCL) for defense contractor personnel and defense contractor facilities. It is one of eight Central Adjudication Facilities (CAF) within DoD.

### **What are the security clearance levels?**

Security clearances can be issued by many United States government agencies, including the Department of Defense (DoD), the Department of Homeland Security, the Department of Energy (DoE), the Department of Justice, and the Central Intelligence Agency. DoE clearances include the "L," and "Q" levels. DoD issues more than 80% of all clearances. There are three levels of DoD security clearances:

- Confidential
- Secret
- Top Secret.

### **What type of information is requested on a security clearance application?**

The application form requires personal identifying data, as well as information regarding residence, education and employment history; family and associates; and foreign connections/travel. Additionally, it asks for information about arrests, illegal drug involvement, financial delinquencies, mental health counseling, alcohol counseling, military service, prior clearances, civil court actions, and subversive activities. The number of years of information required on the form depends on the level of clearance



involved. For instance, residence, education, and employment history for a Top Secret clearance requires ten years of information, whereas a Secret clearance requires seven years.

#### **How long does a clearance remain in effect?**

Generally as long as cleared individuals remain employed by a cleared contractor and are reasonably expected to require access to classified information, their personnel security clearance will remain in effect, provided they comply with periodic reinvestigation requirements.

#### **When is a clearance terminated?**

A clearance is terminated when a person permanently leaves a position for which the clearance was granted. Cleared individuals who no longer require access to classified information, but who remain continuously employed by the same cleared contractor and do not anticipate future access can have their clearances administratively downgraded or withdrawn until such time that they require access again, provided their security investigation has not expired. Under such circumstances the clearance can be administratively restored.

#### **What do the terms "active," "current" and "expired" mean?**

People either have a clearance or they don't have a clearance. The Personnel Security Investigation (PSI) on which the clearance is based can be either "current" or "expired." PSIs are current if they are not more than five years old for a Top Secret clearance, 10 years old for a Secret clearance, or 15 years old for a Confidential clearance. Generally, if the PSI is out-of-date (expired) or there has been a break-in-service of two years or more, a person must be nominated for a new clearance and must complete a new application in the same manner as a person who never had a clearance.

#### **Can a clearance be reinstated after it has been terminated?**

Yes. If a person previously had a clearance and the investigation is still current, the clearance can be reinstated by the agency that originally granted the clearance or it can be accepted and granted by a different agency, provided there hasn't been a break-in-service of two years or more. This usually only entails the submission of a new application and a favorable review of the application by the clearance granting authority.

#### **What is an interim security clearance?**

An interim clearance (also known as "interim eligibility") is based on the completion of minimum investigative requirements and granted on a temporary basis, pending the completion of the full investigative requirements for the final clearance. Interim Secret clearances can be issued rather quickly once the clearance granting authority receives a properly completed application. Interim Top Secret clearances take two or three months longer. Interim clearances can be denied, if unfavorable information is listed on the application form or at any time unfavorable information is developed during the investigation. All applicants are considered for interim clearances by the Defense Industrial Security Clearance Office.

With some exceptions an interim clearance permits a person to have access to classified material at all levels of classification up to the level of the clearance requested. Interim Secret clearances are not sufficient for access to special categories of classified information, such as COMSEC, NATO, and



Restricted Data. Interim Top Secret clearances are sufficient for access to COMSEC, NATO, and Restricted Data at the Secret and Confidential levels only.

## Getting a Clearance

### **Can I obtain a security clearance on my own?**

No. You must be sponsored by a cleared contractor or a government entity. To be sponsored you must be employed by a cleared contractor (or hired as a consultant) in a position that requires a clearance. As an exception, a candidate for employment may be submitted for a clearance if the cleared contractor has made a binding offer of employment and the candidate has accepted the offer. Both the offer and acceptance must be in writing. The offer of employment must indicate that employment will begin within 30 days of receiving the clearance.

### **Can a Naturalized Citizen get a Personnel Clearance?**

Yes. A naturalized citizen is treated the same as a native born US citizen.

### **Can non-US citizens obtain security clearances?**

No. Non-US citizens can not obtain a security clearance; however, they may be granted a Limited Access Authorization (LAA). LAAs are grant in those rare circumstances where the non-US citizen possesses unique or unusual skill or expertise that is urgently needed to support a specific US Government contract involving access to specified classified information (no higher than Secret), and a cleared or clearable US citizen is not readily available.

## Personnel Security Clearances (PCL)

### **Who issues clearances?**

The Defense Industrial Security Clearance Office (DISCO) in Columbus, OH issues DoD contractor Personnel Clearances (PCL). PCLs are based on completed personnel security investigations (PSI) that do not have any serious security or suitability issues. When DISCO is unable to issue a PCL, the case is forwarded to the Defense Office of Hearings and Appeals (DOHA) for further consideration.

### **How much does it cost to get a PCL?**

At this time, there is no direct charge for a PCL issued by DISCO.

### **What is a collateral clearance?**

The term "collateral clearance" is used to describe a security clearance without any special access authorizations.

### **What is a "special access authorization?"**

Access to classified defense information is based on an appropriate level of security clearance (Confidential, Secret or Top Secret) and a "need-to-know." Need-to-know can be either a formal or an informal determination. All classified defense information exists within one of these two "need-to-know" domains—formal or informal. Information that exists within the domain of informal need-to-know determinations is referred to as "collateral classified" information. Information that requires a formal need-to-know



determination (also known as a special access authorization) exists within Special Access Programs (SAP) and Sensitive Compartmented Information (SCI).

Acronyms such as ATOMAL, CNWDI, COMSEC, COSMIC, CRYPTO, NOFORN, ORCON, SAP, SCI, SIOP-ESI, SPECAT, SIOP-ESI, etc., are not clearances. They are categories of classified information, some of which have extra need-to-know restrictions or require special access authorizations. For example, COSMIC stands for "Control of Secret Material in an International Command." COSMIC Top Secret is the term used for NATO Top Secret Information. There are many such markings stamped or printed on classified material, but most are only acronyms denoting special administrative handling procedures.

### **How can I be granted Sensitive Compartmented Information (SCI) access?**

No one is actually granted SCI access, since SCI encompasses several categories of compartmented information. People are granted eligibility for SCI access. Once this eligibility has been established, a person can be granted a special access authorization for a specific category of information within SCI. In order to be considered for SCI access, a cleared individual must first be nominated for an SCI billet and approved by the government agency that controls the information.

### **What is a Special Access Program (SAP)?**

A SAP is defined as: "a program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level." Technically, SCI is a SAP. Some SAPs are referred to as "black" programs; the very existence of which can be classified.

### **Can you get an interim access authorization for SCI/SAP?**

Interim access authorizations for Sensitive Compartmented Information (SCI) and Special Access Programs (SAP) are granted under very limited circumstance through a completely different process than clearances.

## **Clearance Process**

### **What are the steps to getting a Personnel Clearance (PCL)?**

A cleared contractor identifies an employee with a need to have access to classified information (e.g., the employee will work on a classified contract). Once identified, the contractor's Facility Security Officer (FSO) submits an investigation request through the Joint Personnel Adjudication System (JPAS) and ensures that the employee completes a clearance application in the Electronic Questionnaires for Investigations Processing (e-QIP). The FSO then reviews, approves, and forwards the completed e-QIP to the Defense Industrial Security Clearance Office (DISCO) for their approval and release to Office of Personnel Management (OPM). OPM conducts an investigation and sends the results of the investigation to DISCO. DISCO either grants a clearance or forwards the investigation to Defense Office of Hearings and Appeals (DOHA) for further adjudication.

### **How are security clearance investigations carried out?**

The National Agency Check and credit check portions of all investigations are conducted by the Office of Personnel Management (OPM), Federal Investigations Processing Center (FIPC) near Boyers, PA. The Local Agency Check (police records) portion can be done in part by FIPC or completely by field



investigators. For cases requiring other record checks, reference interviews, or a Subject Interview, tasking is sent from FIPC simultaneously to supervisors of field investigators (either federal agents or contract investigators) in all locations involved. If the investigation develops information that requires further action in another location, tasking is sent from the investigative office that developed the information to another field office. Investigative reports are electronically submitted as the work is completed. When all reports have been received a FIPC, the case is reviewed for completeness, then forwarded to the appropriate Central Adjudication Facility (the Defense Industrial Security Clearance Office for DoD industrial clearances).

### **How long does it take to process a security clearance?**

In September 2006 defense contractors reported average end-to-end processing time of over one year for Top Secret clearances.

A February 2007 report by the Security Clearance Oversight Group (SCOG) indicated that it took an average of 205 days for all types of clearances granted by agencies whose investigations were done by the Office of Personnel Management (OPM). This figure was based on investigations completed between October 1, 2006 and February 3, 2007. The report admits that this number does not include the application processing time before an investigation is opened by OPM. In a September 2006 report, GAO calculated this application processing time for Top Secret clearances handled by the Defense Industrial Clearance Office (DISCO) to be about 111 days. The figure in the SCOG report may also be somewhat skewed due to OPM's emphasis on completing cases opened after October 1, 2006. The report did not provide separate figures for different levels of clearances; however, anecdotal information suggests that Confidential and Secret clearances take about two or three months less than Top Secret clearances.

### **Will my clearance be granted faster because I had a clearance three years ago?**

No, not if you previously held a Secret or Confidential clearance. If you previously held a Top Secret clearance and the investigation was completed less than five years ago, it is possible that a very small portion of the new investigation will not have to be repeated.

### **Will my clearance be granted faster, if I have immediate family members who have clearances?**

No.

### **Why does it take so long to get a clearance?**

Part of the answer is that for over a decade insufficient resources have been allocated to clearance processing, causing a large backlog of cases. The other part of the answer involves the applicant and requires a better understanding of the process. There are three phases to clearance processing: 1) application processing, 2) investigation, and 3) adjudication. Most of the delays in getting a clearance are caused by either:

- "queuing" time
- poorly completed security applications
- extended periods of residence outside the United States
- serious security/suitability issues



Delays caused by queuing time (the time a case sits waiting to be acted on) occur in all three phases of processing and affect all cases. A certain amount of queuing time is necessary for efficient operations, but when there is a significant backlog of cases, queuing time becomes excessive. Poorly completed security applications can result in the application processing and investigation phases significantly longer. The other problems only affect the investigation phase but can also increase the length of time for the investigation. A September 2006 General Accountability Office report indicated the following average processing times for initial Top Secret clearances granted by the Defense Industrial Security Clearance Office (DISCO) in January and February 2006:

- Application processing: 111 days
- Investigation: 286 days
- Adjudication: 39 days

The application processing phase was calculated from the date the application was transmitted to DISCO to the date the investigation was opened at OPM. It did not include the time applicants take to complete the application. OPM reports that about 10% of all clearance applications are rejected and returned to the requestor due to incomplete or inconsistent information. No information is available regarding the percentage of applications rejected by DISCO. Personnel in the office of the Undersecretary of Defense for Intelligence estimated that, as of April 2005, between 20 to 25 percent of DoD requests for personnel security investigations were rejected.

Reviews of applications at DISCO and OPM before an investigation is opened can only discover obvious errors and omissions. These reviews do not discover wrong addresses, telephone numbers and dates, nor do they discover omitted foreign travel, relatives, residences, employment or education. These errors and omission are only discovered during the investigation and add a significant amount of work to the case. Poorly completed applications not only delay the application processing and investigation phases; they also contribute to the backlog of cases and to lengthening the queuing time for all clearances.

#### **What can I do to speed up the process of getting a clearance?**

1. Get a paper copy of the application form (Standard Form 86—SF86) at [www.qsa.gov](http://www.qsa.gov). Complete the paper copy of the SF86, before attempting to complete the electronic (eQIP) version online. You will save yourself a lot of time and frustration.
2. Provide complete and accurate information. Too often applicants fail to list short-term employment, residence, education, and other seemingly unimportant information. When an investigation turns up missing or discrepant information, it adds extra time to the investigation.
3. Postal Zip Codes are critical. A wrong Zip Code will result in part of your investigation being sent to the wrong investigative office, and the case could languish for weeks before the error is noticed. Get Zip Codes at <http://zip4.usps.com/zip4/welcome.jsp>.
4. Get a free credit report from [www.annualcreditreport.com](http://www.annualcreditreport.com) and review it before completing an SF86. Something you were unaware of may appear on the report and cause delays.



5. When entering the "Name of Person Who Knew You" in the Residence Section of the SF86, list neighbors. Avoid listing relatives in any section of the SF86, except Section 13—Spouse and Section 14—Your Relatives And Associates.
6. Don't indicate dual citizenship just because you were born in a foreign country, unless you are certain you have dual citizenship. Go to [www.opm.gov/extra/investigate/IS-01.pdf](http://www.opm.gov/extra/investigate/IS-01.pdf) and check the citizenship laws of foreign county where you were born.
7. If you have a foreign passport due to dual citizenship, indicate in the Comment Section of the SF86 your willingness to surrender it to the proper authorities. Do not contact any foreign official regarding the passport or citizenship, unless you are instructed to do so by a representative of the U.S. Government.
8. If you had mental health or substance abuse counseling in the past 7 years, contact the facility where the counseling occurred and determine if they will accept a standard government release for medical information. If not, get a blank copy of their release and take it with you to your personal interview.
9. If you left a job under less than favorable circumstances, explain the situation in the comment section of Question 22 of your SF86, and give the name and/or position of the person who terminated you or asked you to quit.
10. Couch any unfavorable security and suitability information in terms directly applicable to the mitigating conditions listed in the Adjudicative Guidelines. The most recent version of the "Adjudicative Guidelines for Determining Eligibility for Access to Classified Information" was issued on December 29, 2005. There are 13 guidelines covering such things as alcohol consumption, drug involvement, financial considerations, criminal conduct, etc. Each explains potential disqualifying conditions and mitigating conditions.

#### **Who should I list as references on my clearance application?**

There are 4 sections of the clearance application ("Where You Have Lived," "Where You Went To School," "Your Employment Activities," and "People Who Know You Well") that require names and contact information for people who can be interviewed as references. Unless there is no other choice, do not list any relatives in these sections. For your residences you should list current and former neighbors. For employment you should list current and former supervisors. If you believe the investigator will have trouble locating a former supervisor, list a former coworker instead. For schools you should list former schoolmates or faculty members who will remember you. For "People Who Know You Well" try to list at least one person who has known you for the past seven years and who knows who your other friends are. Try not to list the same person more than once on your clearance application.

#### **Will I be interviewed by an investigator?**

If you are being investigated for a Top Secret clearance or for a Secret clearance that requires access to a designated Special Access Program (SAP), a Personal Subject Interview (PRSI) is a regular part of the investigation. A Special Interview (SPIN) can be required in any investigation, if a previously undisclosed suitability/security issue surfaces. SPINs can also be required in an investigation for a Confidential or Secret clearance, if a suitability/security issue is listed on your clearance application.



### **What will I be asked during a security clearance interview?**

During a PRSI, the investigator will cover every item on your clearance application and have you confirm the accuracy and completeness of the information. You will be asked about a few matters that are not on your application, such as the handling of protected information, use of information technology systems, and sexual misconduct. You will be asked to provide details regarding any potential security/suitability issues.

During a SPIN, the investigator will only cover the security/suitability issue(s) that triggered the SPIN. The purpose of the SPIN is to afford the applicant the opportunity to refute or to confirm and provide details regarding the issue(s).

### **Should I reveal unfavorable information about myself on the clearance application?**

Yes. The majority of clearance denials for drugs, alcohol, and criminal conduct also involve providing false information during the clearance process. In many cases the misconduct people try to hide probably would not result in a clearance denial. Passage of time is a major mitigating factor for all issues involving misconduct. Willfully providing false information on a clearance application or during a Subject Interview is judged under two separate Adjudicative Guidelines—Personal Conduct and Criminal Conduct—and is of such recency that mitigation is almost impossible. Without mitigation any serious criminal conduct or false official statement can result having your clearance denied.

### **What are the most common errors requiring correction before the investigation is opened?**

- Incomplete addresses for residence, employment, and education.
- Incomplete information regarding delinquent debts (no explanation in comment section).
- Releases not signed, dated, or legible.
- Name on application does not exactly match name on fingerprint card.
- Date of birth and place of birth differences between application and fingerprint card.
- Lack of social security number and place of birth for cohabitant on SSBI requests.
- If legally separated from spouse, lack of address for spouse and date of separation.

### **How can I find out the status of my clearance application?**

Only your Facility Security Officer (FSO) may inquire about the status of your security clearance application. The FSO can do this by checking the Joint Personnel Adjudication System (JPAS) and/or the Security and Investigations Index (SII) or by telephoning the DoD Security Service Center at 888-282-7682.

### **How will I be informed when I am granted a clearance?**

Normally you will be contacted by a representative of your Facility Security Officer and required to sign a "Classified Information Non-disclosure Agreement" and a form acknowledging that you have received a security briefing, prior to be granted access to classified information.

### **What types of things can prevent someone from receiving a security clearance?**

With rare exceptions the following will result in a clearance denial:

- criminal conviction resulting in incarceration for a period of one year or more



- current unlawful use of or addiction to a controlled substance
- determined to be mentally incompetent by a mental health professional approved by DoD
- discharge or dismissal from the Armed Forces under dishonorable conditions
- unwillingness to surrender a foreign passport

Otherwise, the most common reasons for clearance denial are serious repeated financial problems, intentional false statements in connection with a clearance investigation, recent illegal drug involvement, repeated alcohol abuse, and a pattern of criminal conduct or rule violation. For most people these issues can be mitigated, if presented properly during a security interview.

The 2005 “Adjudicative Guidelines for Determining Eligibility for Access to Classified Information” list various conditions under 13 separate guidelines that could result in clearance denial.

### **What happens when a security clearance is denied?**

When a case contains significant derogatory information, it is forwarded from the Defense Industrial Security Clearance Office (DISCO) to the Defense Office of Hearings and Appeals (DOHA). DOHA adjudicators can send the case back to DISCO with instructions to grant the clearance or DOHA can issue a “Letter of Intent” (LOI) to deny a clearance. The LOI is a preliminary, tentative decision and will contain a “Statement of Reasons” (SOR) detailing the issues that are the basis of the decision. The applicant can make a written rebuttal to the SOR and request a hearing. If the applicant does not rebut the SOR, DOHA will direct DISCO to deny the clearance. If the applicant rebuts the SOR without request a hearing, DOHA sends the applicant all relevant and material information that could be presented to a DOHA Administrative Judge (AJ) for a clearance decision based on the written record. The applicant can submit a written response to this information. If the applicant requests a hearing, the applicant may present witnesses and other evidence. The applicant may also cross-examine witnesses and challenge evidence presented by the DOHA Department Counsel. The AJ makes a written decision and a copy is given to the applicant. DISCO is then directed to grant or deny the clearance in accordance with the AJ’s decision.

### **Can I appeal a clearance denial or revocation?**

An applicant may appeal an adverse decision by the DOHA Administrative Judge (AJ) by filing a notice of appeal. The applicant must then submit a written appeal brief. The appeal brief is reviewed by the Appeal Board at DOHA. An appeal can only be based on an error made by the AJ. No new evidence can be submitted.

### **What is the EPSQ (Electronic Personnel Security Questionnaire)?**

Until July 2005, the EPSQ was the only electronic security clearance application used within the National Industrial Security Program (NISP).

### **What is e-QIP (Electronic Questionnaire for Investigations Processing)?**

e-QIP is an Office of Personnel Management (OPM) web-based computer program in which an applicant enters the same information as required on the Standard Form 86—Questionnaire for National Security Positions. e-QIP became available in July 2005 and has been slowly replacing the EPSQ. OPM anticipates that 100% of clearance applications from all major requestors will be submitted using e-QIP by the end of 2007.



### What is JPAS (Joint Personnel Adjudication System)?

JPAS is the official personnel security clearance database management system for DoD and other government users. All National Industrial Security Program (NISP) cleared contractors use this system for all types of personnel clearance actions, including initiating requests for clearance investigations. For more information, visit the JPAS website at <https://jpas.dsis.dod.mil/>

### How can I get a copy of my clearance investigation?

First you must determine who conducted your investigation. The Defense Security Service (DSS) and the Office of Personnel Management (OPM) have conducted ninety percent of all clearance investigations over the past 35 years.

For OPM investigations mail or fax a request with your hand written signature to:

FOI/P, OPM-FIPC  
P.O. Box 618  
1137 Branchton Road  
Boyers, PA 16018-0618  
FAX: 724-794-4590

Include the following information in your request:

- Full name
- Social Security Number
- Date of birth
- Place of birth
- Current home address (a Post Office Box is not acceptable; the records are sent by certified mail and require your signature).

For DSS investigations mail a written request with your original notarized signature to:

Defense Security Service  
Privacy Act Branch  
938 Elkridge Landing Road  
Linthicum, MD 21090-2917

Include the following information in your request:

- Full current name
- Any other names you may have used in the past
- Date of Birth
- Social Security Number
- A brief description of the records you are seeking



- Any other information that you believe may be useful in searching for records pertaining to you

Additionally, due to the transfer of the personnel security investigations function to OPM on February 20, 2005, any requests for DSS investigations completed after February 20, 2005 should be mailed to the OPM. DSS only maintains those personnel security investigations completed by DSS prior to the February 20, 2005, transfer.

## Polygraphs

### **What are polygraphs?**

Polygraphs are instruments that measure physiological responses (respiration, pulse, blood pressure, and galvanic resistance) to stress. Polygraphs are used to help determine an individual's eligibility for a special assignment or access to specifically designated information protected within SAPs. They are not generally used for collateral security clearances, unless they are necessary to resolve serious credible derogatory information that can not be resolved through conventional investigative means. Polygraph examinations are conducted as a supplement to, not as a substitute for, other forms of investigation that may be required under the circumstances. Polygraphs exams are only administered by agencies with approved personnel security polygraph programs, and these exams are only conducted by government trained and certified examiners.

### **What are the differences between Counterintelligence, Lifestyle, and Full Scope Polygraphs?**

Within the context of security clearances, the purpose of a polygraph exam is to assist in determining whether or not an applicant can be trusted with sensitive information. For screening purposes two types of polygraph exams exist, and either one or both exams may be administered.

A Counterintelligence Polygraph asks the candidate questions limited to those necessary to determine whether the examinee ever had any involvement with or knowledge of espionage/sabotage against the United States, unauthorized contact with representatives of a foreign government, or unauthorized disclosure of classified material. A Counterintelligence Polygraph is the most common polygraph. Within DoD, polygraph examinations used to determine initial eligibility for special assignment or special access are limited to counterintelligence questions.

A Lifestyle Polygraph asks the candidate questions that concern the subject's personal life and conduct and can involve all aspects of present and past behavior. Questions asked might concern drug and alcohol use, sexual misconduct, mental health, family relationships, compulsive or addictive behavior, and more. A Lifestyle Polygraph attempts to look for issues in a person's private life for which he or she might be susceptible to blackmail or coercion.

A Full Scope Polygraph is a combination of both the Counterintelligence and Lifestyle polygraphs.

## Types of Investigations

**National Agency Check with Local Agency Checks and Credit Check (NACLC)**



A NACLCL is the type of investigation required for a Secret or Confidential clearance. It includes a credit bureau report and a review of records held by federal agencies and by local criminal justice agencies. It generally does not require an interview with an investigator. The investigation routinely covers no more than the past seven years of a person's life or a shorter period if the applicant is less than 25 years old.

### **Single Scope Background Investigation (SSBI)**

An SSBI is a more detailed investigation and is required for a Top Secret clearance, for Sensitive Compartmented Information (SCI) access, and for designated Secret Special Access Programs (SAP). It includes a NACLCL, a Personal Subject Interview (PRSI), interviews of former spouses; interviews of character, employment, neighborhood, and educational references; reviews of rental, employment, and academic records. The investigation routinely covers no more than the past 10 years of a person's life or a shorter period if the applicant is less than 28 years old.

### **Periodic Reinvestigation (PR)**

People with security clearances must be routinely reinvestigated at set intervals based on the level of clearance they possess. A Periodic Reinvestigation is done to ensure that cleared personnel are still suitable for access to classified information. The type of reinvestigation and frequency required depend on the level of clearance:

- Top Secret requires an SSBI-PR or PPR every 5 years.
- Secret requires an NACLCL every 10 years.
- Confidential requires an NACLCL every 15 years.

### **SSBI-PR (Single Scope Background Investigation—Periodic Reinvestigation)**

An SSBI-PR includes an NACLCL, Personal Subject Interview, references interviews, and record reviews covering at least the past five years.

### **PPR (Phased Periodic Reinvestigation)**

In September 2005 OPM made the PPR available as a less comprehensive and less expensive alternative to the SSBI-PR. The investigation includes an NACLCL, Personal Subject Interview, and limited reference interviews and record reviews. PPRs may not be requested when certain questions on the clearance application contain responses indicating a possible security or suitability issue.

### **Reimbursable Suitability Investigation (RSI)**

The RSI consists of a focused investigation to provide additional specific information to resolve developed issue(s) that fall outside the scope of coverage of other investigative products offered by the Office of Personnel Management (OPM).

### **Trustworthiness Investigation**

Trustworthiness investigations are not conducted for a security clearance. It is requested when an applicant is going to have access to Sensitive but Unclassified Information or occupy a position of "Public Trust." For example, trustworthiness investigations are sometimes conducted on those that will have access to a sensitive site (e.g., cleaning crew on a military installation).



## **Other Investigations**

The Office of Personnel Management (OPM) conducts other types of investigations. Some are for employment purposes only, and others are for a combination of employment and security clearance purposes. These investigations are generally not conducted for the Department of Defense contractor personnel.

## **Facility Security Clearances (FCL)**

### **What is the National Industrial Security Program (NISP)?**

The NISP is the industrial security program that governs the contractual security obligations of DoD contractors and contractors of 23 other federal government participants. The Defense Security Service (DSS) has primary responsibility for monitoring NISP compliance. All NISP requirements are contained in the National Industrial Security Program Operating Manual (NISPOM) and NISPOM supplements.

### **How does a company get a facility clearance (FCL)?**

A company must be sponsored for an FCL by a government agency or a cleared contractor. A company cannot sponsor itself for an FCL. The cleared contract or government agency requests the FCL when a definite, classified procurement need has been established.

### **How does a contractor sponsor a company for a FCL?**

Sponsorship is in the form of a letter to the Defense Industrial Security Clearance Office (DISCO) requesting that a particular company be processed. The letter provides the prospective company's name, address, phone number and point of contact. It should also provide the contract number for the classified procurement, a copy of the Contract Security Classification Specification, facility clearance level needed and the requestor point of contact and phone number.

### **What is a Contract Security Classification Specification, DD Form 254, and how does it relate to a FCL?**

A DD Form 254 is issued when classified work is contracted to a facility. It provides the security classification and safeguarding requirements to be applied to information. The government agency or cleared contractor issues the 254 to the contracted facility and justifies the need for a FCL. One or more active DD Form 254 is necessary to maintain an active FCL. The DD Form 254 will determine the level of the FCL granted to the company. A company's FCL level must be as high as the highest classification specified in any of its DD Forms 254.

### **What is a DSS Industrial Security Representative (IS Rep.)?**

Once sponsored for a FCL, contractors are assigned an IS Rep (a DSS employee). The IS Rep's job is to assist the contractor in following the regulations of the NISPOM the entire time it is a NISP participant.

### **What is a DSS inspection/review?**

A DSS review is a periodic visit by a DSS IS Rep. The review is conducted to assist the contractor in following the requirements of the NISPOM and ensure that safeguards employed by the contractor are adequate for the protection of classified information. The IS Rep determines the frequency of such formal reviews, but reviews are normally conducted annually.



### **Who has to be cleared in connection with a FCL?**

A DSS Industrial Security Representative (IS Rep) with the help of the company's POC will determine which individuals must be cleared in connection with the FCL. Ordinarily, those who have control over the company (e.g., owners, officers, directors, and executive personnel) and the Facility Security Officer (FSO) must be cleared. Those individuals cleared in connection with a FCL are called Key Management Personnel (KMP).

### **What happens if a "controlling" officer cannot be cleared in connection with the FCL?**

The facility is not eligible for a FCL. The National Industrial Security Program Operating Manual (NISPOM) has provisions for "excluding" certain KMP (but not the senior management official or FSO), if they are unable to obtain a clearance. Under this provision there must be a resolution by the company's executive body (e.g., Board of Directors) that the named individual will not be provided any classified information, can be effectively excluded from access to all classified information, and is not in a position to adversely affect the performance of the classified contract. Alternatively, the officer can officially step down from his or her title as an officer/director and relinquish control of the facility.

### **What is a Facility Security Officer (FSO)?**

The FSO is a KMP who has responsibility over the facility's security program. During the time in which a facility is cleared, the FSO is the main POC for the DSS IS Rep.

### **Does the FSO have to have a personnel clearance? What level?**

Yes. The FSO must have a clearance at the same level as the FCL.

### **How does a company get a Top Secret FCL?**

A company must be sponsored for a Top Secret FCL, even if it already has a lower level FCL. A cleared contractor or government agency must follow the same sponsorship procedures and personnel clearances for all KMPs must be upgraded as well.

### **How much does it cost to get a FCL?**

At this time, there is no direct charge for a FCL issued by Defense Industrial Security Clearance Office (DISCO).

### **What is FOCI (Foreign Ownership, Control or Influence)?**

A contractor is determined as having FOCI when under such a level of foreign control or influence that it cannot be cleared without a negation method. DSS assists the contractor in selecting a negation method; however, some levels of FOCI cannot be negated and the contractor is determined ineligible for an FCL.

### **What are SCIFs and SAPF?**

A SCIF (Sensitive Compartmented Information Facility) and a SAPF (Special Access Program Facility) are specially constructed facilities to safeguard SCI and SAP information.

### **Who inspects SCIFs and SAPFs?**



DSS is responsible for inspections of these facilities, unless they have been specifically “carved out” of the NISP by the government customer. In which case the government customer who approved the facility and owns the information inspects the facility.

## Security Clearance Jobs

### **Where can I search for jobs that require a security clearance?**

Candidates with active clearances and those with clearances that can be reinstated can search for jobs that make use of that clearance at ClearanceJobs.com (<http://www.clearancejobs.com>).

### **If I don't have a security clearance, where can I find employers that might be able to sponsor me to receive one?**

Candidates without clearances can search for jobs that do not require clearances at other Internet-based job boards like Dice.com (for IT candidates), Monster.com (all professions), and HotJobs.com (all professions).

## Security Clearance History Timeline

### **Why is there a clearance backlog? How can I better understand the course of events that have shaped the personnel security clearance investigation process?**

The history is fairly long and complicated. However, certain specific events give a clear understanding of how the security clearance investigation process has evolved, and the difficulties the US Government has faced. In general, five types of problems have caused the security clearance backlog to remain at large numbers.

1. Increase of new personnel clearance requests and periodic reinvestigations
2. Failure of DoD requestors to accurately estimate the number of clearance requests
3. Inadequate resources and personnel for Defense Security Service
4. Frequent changes in leadership positions at Defense Security Service
5. Problems shifting responsibility from Defense Security Service to Office of Personnel Management

The timeline below can help understand the challenges the US government faces.

### **DoD Personnel Clearance Backlog Timeline**

- |             |   |
|-------------|---|
| <b>1981</b> | General Accounting Office (GAO) reported to Congress that nearly a billion dollars was wasted annually because of investigative backlogs at the Defense Investigative Service and recommended increasing their budget (Defense Security Service was known former known as the Defense Investigative Service). |
| <b>1989</b> | Defense Security Service (DSS) hits high point of 3,100 personnel involved in Personnel Security Investigations (PSI), including about 2,400 field investigators.   |



- 1991** A 40% downsizing of DSS begins. DSS completes 923,000 investigations with an average turnaround time for all investigations of about 50 days.
- Oct 1991** President signs National Security Directive 63 mandating the Single Scope Background Investigation (SSBI) for Top Secret Clearances; amount of work for Top Secret clearance investigations increases substantially.
- Jan 92** Revision of Director of Central Intelligence Directive 1/14 adds neighborhood investigations to Periodic Reinvestigations (PR) for Top Secret clearances.
- 1992** DSS underestimates number of PRs for Secret clearances and the increased workload caused by the SSBI. Secret-PRs increased from about 36,000 in 1991 to 93,000 in 1992).
- 1993** DSS personnel involved in Personnel Security Investigations (PSI) shrinks to 2,586, including about 2,000 field investigators.
- Feb 1994** Joint Security Commission issues report recommending standardization, computerization, and changes in investigative scope. It also recommends that DSS change from appropriated funding to fee-for-service.
- Aug 1995** New Personnel Security Executive Order 12968 mandates change and standardization of investigative scope.
- 1996** Number of DSS field investigators shrinks to about 1,250, plus about 350 supervisors and support personnel. This number remains about the same until transfer to Office of Personnel Management (OPM) in February 2005.
- 1996-1998** New DSS Director - Marge Munson
- 1996-1999** Quotas for Periodic Reinvestigations implemented, resulting in a decrease of incoming cases but an increase in the backlog growth.
- Mar 1997** DSS eliminates all first-line investigative supervisor positions and increases supervisory span of control from about 1:10 to about 1:25.
- Mar 1997** Full implementation of 1995 EO 12968 delayed.
- 1998-1999** New DSS Director - Steve Schanzer
- Mar 1998** Information Security Oversight Office (ISOO) promulgates new standards required by 1995 EO 12968. NACLIC becomes standard for Secret and Confidential initial clearances and periodic reinvestigations (PR). PRs for these clearances are set at 10- and 15-year intervals. Single Scope Background Investigation-Periodic Reinvestigation (SSBI-PR)



becomes standard for Top Secret periodic reinvestigations at 5-year intervals. SSBI for initial Top Secret clearances remains unchanged.

- Apr 1998-1999** Government Accountability Office (GAO) initiates a 16-month audit of the Defense Security Service and its backlog.
- Oct 1998** Use of Case Control Management System (CCMS), new computer program and database for processing investigations at Defense Security Service (DSS) begins. Old system is turned off and performance decreases significantly.
- Jan 1999** Full implementation of Executive Order 12968; backlog of Periodic Reinvestigations increase to 400,000
- 1999-2002** New DSS Director - General Charles Cunningham
- Mar 1999** Defense Security Service performance decreases—situation worse than originally reported to Department of Defense.
- 1999** Office of Personnel Management begins assisting Defense Security Service with Personnel Clearance investigations.
- Jun 1999** DSS Director Cunningham provides recovery plan by using additional investigative resources (reservists, contractors, Office of Personnel Management).
- Aug 1999** Joint Security Commission II reports 700,000 people with clearances are past due for periodic reinvestigations.
- Oct 1999** All DoD civilian employee security clearance investigation requests are sent to Office of Personnel Management for processing.
- Oct 1999** General Accountability Office releases report charging that completeness and timeliness problems in DoD's personnel security program resulted largely from a series of Defense Security Service (DSS) management actions that weakened quality assurance and led to delays in processing cases. Specifically, DSS:
- adopted relaxed investigative policy guidance causing confusion about investigative requirements and raising concerns about the sufficiency of information available for clearance decisions and the impact on uniformity in all personnel security investigations;
  - eliminated quality control mechanisms such as quality assurance and supervisory review of completed investigations;



- ineffectively managed implementation of a new automated investigative case processing system that caused delays in processing cases; and
- did not adequately train its staff on the new federal investigative standards, causing much confusion among DSS staff about conducting investigations in compliance with the federal standards.

**Mar 2000** DoD reports backlog of 505,000. Cunningham promises to get backlog under control by 2001; reports reason for the backlog is threefold: requirements for PRs were tightened in 1997 increasing the number due, the agency was downsized by 40%, and in 1998 CCMS, a new DSS computer program for managing Personnel Security Investigations, did not work because the design was inadequate.

**Mar 2000** Deputy Secretary of Defense approves transfer of 800,000 investigations from DSS to OPM over a 2-year period.

**Apr 2000** Senate Armed Services Committee meeting; cost of DSS backlog is more than \$100 million; DSS Director Cunningham reported that he inherited an incompetent agency

**Aug 2000** GAO reports a backlog of 500,000 cases.

**Aug 2000** DSS reports that its \$100 million computer system (CCMS) shutdown for more than a week due to overload; DSS Director Cunningham reported that the backlog would not be reduced until 2002.

**Sep 2000** Subcommittee chairman, Chris Shays, R-Conn, states that the clearance system is a "mess."

**Dec 2000** DoD reports a backlog of 317,000.

**Mar 2001** Cunningham reports to a House of Representatives hearing that DSS has "turned the corner and can demonstrate a noticeable decrease in the backlog."

**Mar 2001** DSS reports that there are 188,000 cases loaded in CCMS but not opened due to limitations of the system; cases will be opened by August 2001.

**Oct 2001** DoD reports that once implemented, Joint Personnel Adjudication System (JPAS) will help reduce the backlog.

**May 2002** DSS Director Cunningham retires; DSS headed by Acting Directors William Curtis (2002-2004) and Heather Anderson (2004-2005)

**Jan 2004** Defense Authorization Bill—DoD authorizes the transfer of DSS PSI functions to OPM.



- Feb 2004** GAO Report to Committee on Armed Services, House of Representatives, "Department of Defense Personnel Clearances"
- DSS did not know size of backlog; had not estimated it since January 2000. Reasons for backlog:
- increased number of requests
  - decreased number of agents
  - size of backlog
  - lack of strategic plan to reduce the backlog
  - inadequate Department of Defense oversight
  - delays in implementing JPAS
- Feb 2004** DSS and OPM state a need for additional resources; they currently have only half of investigators needed.
- May 2004** House Govt. Reform Committee Hearing:
- GAO reports backlog is 360,000
  - DSS reported a need for 8000 investigative personnel; current number is 5300
  - Largest impediment is that DSS began sending investigators overseas to help military with its Personnel Security Investigations
  - DSS predicts that all prior year cases will be completed by Sept. 2004 and that no cases will be older than a year
- May 2004** Department of Defense reports a backlog of 434,000.
- May 2004** OPM holds off on merger due to the differences between the agencies in the Personnel Clearance process.
- Nov 2004** DoD "officials" report a backlog of 500,000; Rep. Tom Davis requests that DoD and OPM take immediate steps to reduce the backlog.
- Dec 2004** Intelligence Reform and Terrorism Prevention Act (IRTP) enacted. Title III of IRTP creates an interim goal of December 2006 for getting the clearance backlog under control by requiring that 80% of PSIs be completed within 90 days and adjudicated within 30 days. The IRTP further requires that by Dec 2009 PSIs be completed within 40 days and adjudicated within 20 days.
- Dec 2004** President approves use of Phased Periodic Reinvestigations for Top Secret clearances.
- Jan 2005** Government Accountability Office designates DoD's personnel security clearance program as a high-risk area.

- Feb 2005** Defense Security Service transfers its PSI function and about 1600 personnel to Office of Personnel Management. They join about 4,200 contract investigators and field support personnel already working for OPM
- Jun 2005** E.O. 13381 designates the Office of Management and Budget (OMB) as the element of the executive branch responsible for oversight of all investigations and adjudication for personnel security clearances, including highly sensitive programs, throughout the United States Government. OMB further designates OPM as primary investigative agency for conducting PSIs in the federal government.
- Jun 2005** Oversight of Government Management, Federal Workforce and DC Committee on House and Governmental Affairs Hearing:
- GAO reports that it is not aware of any progress Defense Security Service has made in its 2004 recommendations
  - GAO doubts that the transfer to Office of Personnel Management will help since the Pentagon has continuously underestimated the number of clearances needed each year; also Department of Defense and Office of Personnel Management are unable to connect their computer systems
  - Chairman Voinovich intends to "fix" the security clearance problem; requested that OMB assist with the problem
- Sep 2005** OPM announce availability of the "Phased Periodic Reinvestigation" as a less expensive alternative to the Single Scope Background Investigation-Periodic Reinvestigation (SBI-PR).
- Nov 2005** Janice Haith named new Director of DSS.
- Nov 2005** OPM estimates it will receive about 1,400,000 investigative requests (including 550,000 for security clearances) during FY 2006. OPM reports it has total investigative staff (investigators and support personnel) of 8,400.
- Feb 2006** OMB issues first report to congress in compliance with Title III of the IRTPA, indicating that initial clearance processing time was reduce by 6% (18 days) from Sep 05 to Dec 05, but interprets IRTPA requirements as applying only to initial clearances.
- Mar 2006** OPM reports they now have a combined total (federal and contractor) of about 6,500 field staff involved in Personnel Security Investigations.
- Apr 2006** DoD Inspector General reports serious problems in security clearance application processing at the requesting agency level that result in significant delays before investigations are opened at OPM.

- May 2006** DSS stops processing new industry security clearance investigations and reinvestigations because funds for FY 2006 are exhausted.
- May 2006** DSS obtains additional funds and resumes Secret level clearance processing.
- May 2006** OPM revises estimate from 1,400,000 to 1,700,000 investigative requests (including about 700,000 for security clearances) for FY 2006.
- June 2006** Kathleen Watson named Acting Director of DSS.
- July 2006** DSS obtains additional funds and resumes processing all requests for investigations.
- Sep 2006** GAO analysis of SSBI and SSBI-PRs adjudicated at DISCO from January to February 2006 indicates an average of 446 days for an initial Top Secret Clearance and 545 days for a Top Secret clearance update.
- Jan 2007** OPM reports they now have a combined total (federal and contractor) of about 7,300 field staff involved in PSI.
- Feb 2007** Kathleen Watson named Director of DSS.
- Feb 2007** Security Clearance Oversight Group (SCOG) issues annual report to congress as required by Title III of the IRTPA. SCOG interprets IRTPA interim requirements to apply only to initial clearance investigations opened on or after December 17, 2006, but uses figures based on initial cases opened after October 1, 2006 in their report. The report states that as of February 3, 2007, 64% of the 49,633 initial clearance investigations initiated by OPM during October 2006 have been completed and projects that the December 2006 interim IRTPA requirements will be met.
- Apr 2007** Director of National Intelligence (DNI) announces 100-Day Plan that includes development and implementation of security clearance process improvements, both within the Intelligence Community and at the national level.
- May 2007** OPM reports to Congress of significant progress being made in timely background investigations. The inventory of investigations has been reduced from 385,695 in October 2006 to 100,869 in April 2007. OPM completed 80% of the 137,925 initial clearance investigations received in the first quarter of FY 2007 (October 2006 to December 2006) in an average of 78 days. OPM received 1.7 million background investigations (for employment and security clearances) in FY 2006.

