Security Clearance Frequently Asked Questions

Questions and answers related to US Government security clearances, including those administered under 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. The term "eligibility for access" means the same thing as security clearance and appears in some Government record systems. There are two types of clearances: Personnel Security Clearances (PCLs) and Facility Security Clearances (FCLs).

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. DoD, which issues more than 80% of all clearances, and most other agencies have three levels of security clearances:

- Confidential
- Secret
- Top Secret

DoE primarily issues "L," and "Q" Access Authorizations, which are roughly equivalent to Secret and Top Secret clearances, respectively.

What was DISCO and DOHA?

The Defense Industrial Security Clearance Office (DISCO) was part of the Defense Security Service (DSS), an agency of the Department of Defense (DoD). DISCO processed and adjudicated Personnel Security Clearances (PCL) and Facility Security Clearances (FCL) for defense contractor personnel and defense contractor facilities. The Defense Office of Hearings and Appeals (DOHA) worked with DISCO and adjudicated the most problematic DISCO cases. Previously DISCO/DOHA was one of nine Central Adjudication Facilities (CAFs) within DoD.

What is DoDCAF?

In summer 2011 all nine DoD Central Adjudication Facilities relocated to a new building on Fort Meade, Md. Between August 2012 and January 2013 six of these CAFs (Army CCF, DoNCAF, AFCAF, JCSCAF, WHSCAF, and DISCO/DOHA consolidated into one DoDCAF. The new CAF will have full operational capability by September 2013, including responsibility for Employment Suitability and HSPD-12 credentialing determinations. There has been no decision regarding consolidation of the remaining three CAFs (NSA, DIA, and NGA). They will continue to remain separate entities while the matter is being studied.

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

The application form, Standard Form 86—SF86 (Questionnaire for National Security Positions), requires personal identifying data, as well as information regarding citizenship, residence, education, and employment history; family and associates; and foreign connections/travel. Additionally, it asks for information about

criminal records, illegal drug involvement, financial delinquencies, mental health counseling, alcohol-related incidents and counseling, military service, prior clearances and investigations, civil court actions, misuse of computer systems, and subversive activities. The number of years of information required on the form varies from question to question—many require 7 years, some require 10 years, and others are not limited to any period of time.

How long does a clearance remain in effect?

Generally as long as cleared individuals remain employed by a cleared contractor or government agency 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 (or government agency) 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 clearance 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, complete a new application, and undergo a new PSI. People commonly use the terms "active," "current," and "expired" to mean:

Active—a clearance that has not been terminated.

Current—a terminated clearance that is still eligible for reinstatement.

Expired—a terminated clearance that is no longer eligible for reinstatement.

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 reciprocally granted by a different agency, provided there hasn't been a break-in-service of two years or more. This can be done without the individual submitting a new SF86; however, for clearances involving special access authorizations a new SF86 can be required if there has been a break-in-access of more than 60 days or if a polygraph examination is required.

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 granted in a few days once the clearance granting authority receives a properly completed SF86. Interim Top Secret clearances take one or two months longer. Interim clearances can be "declined," if unfavorable information is listed on the SF86. All industrial applicants

(defense contractor personnel) are considered for interim clearances. Interim clearances can be withdrawn at any time significant unfavorable information is developed during the investigation. It is not possible to appeal the declination or withdrawal of an interim clearance, and the CAF is not required to provide a reason for the declination/withdrawal. Effective 1 August 2012 the term "declined" was replaced by the term "Eligibility Pending," which has the same effect as the declination of an interim clearance.

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 interim clearance granted. Interim Secret clearances are not sufficient for access to special categories of classified information, such as COMSEC, Restricted Data, and NATO. Interim Top Secret clearances are sufficient for access to most Top Secret information and 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 agency. To be sponsored you must be employed (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 employer has made an offer of employment and the candidate has accepted the offer. Both the offer and acceptance must be in writing. The offer of employment from a cleared contractor must indicate that employment will begin within 30 days of receiving the clearance.

Can a Naturalized Citizen get a Personnel Clearance?

Yes. The source of US citizenship does not make a difference for security clearance eligibility.

Can non-US citizens obtain security clearances?

No. Non-US citizens cannot 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 requirement 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 Department of Defense Central Clearance Facility (DoDCAF) at Fort Meade, Md. issues Personnel Clearances (PCL) for most DoD civilians, military personnel, and contractor personnel. Previously the DISCO issued clearances to most defense contractor personnel; however, DISCO was consolidated into DoDCAF in October 2012. Other DoD agencies that issue clearances are DIA, NGA, and NSA. Other Executive Branch departments that issue PCLs include the departments of Energy, State, Homeland Security, Transportation, Agriculture, Labor, Commerce, Treasury, Justice, Interior, Housing and Urban Development, Veterans Affairs, Health and Human Services, and Veterans Affairs. Many component agencies of these departments, as well as independent agencies (i.e. CIA, OPM, EPA, GAO, FCC, USITC, etc.), issue clearances. Clearance determinations are based on completed personnel security investigations (PSI) using the "Adjudicative Guidelines for Determining Eligibility for Access to Classified Information."

How much does it cost to get a PCL?

At this time, there is no direct charge for a PCL issued by DoD and most other federal agencies.

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), including Sensitive Compartmented Information (SCI) and Restricted Data (RD).

Acronyms such as ATOMAL, CNWDI, COMSEC, COSMIC, CRYPTO, NOFORN, ORCON, SAP, SCI, RD, 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 (caveats) 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?

Since SCI encompasses several categories of compartmented information, CAFs grant eligibility for access to SCI. In order to be considered for SCI eligibility, a cleared individual must first be nominated for an SCI billet and approved by the government agency that controls the information. Once this eligibility has been established, a person can be granted a special access authorization for a specific category of information within SCI. SCI access eligibility is divided into 3 sensitivity levels and each has a different investigative requirement:

- SSBI without polygraph
- SSBI with Counterintelligence Scope polygraph
- SSBI with Full Scope polygraph

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 eligibility for access for SCI/SAP?

Interim access eligibility for Sensitive Compartmented Information (SCI) and Special Access Programs (SAP) are granted under very limited circumstances.

Clearance Process

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

For DoD clearances a cleared contractor or Government agency identifies an employee with a need to have access to classified information. Once identified, the contractor's Facility Security Officer (FSO) or the Government agency's Security Officer (SO) 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 or SO then reviews, approves, and forwards the completed e-QIP to the DoDCAF for their approval, issuance of an interim clearance, and release to Office of Personnel Management (OPM). OPM conducts an investigation and sends the results of the investigation to DoDCAF. DoDCAF either grants a clearance or issues a Letter of Intent to deny clearance. Clearances for other federal agencies are processed in essentially the same manner, but can involve a different Investigation Service Provider (ISP).

How are security clearance investigations carried out?

A National Agency Check (NAC), police record checks, and credit check are components of all clearance investigations. When possible these are done centrally by an Investigation Service Provider (ISP), like OPM. Some police record checks must be done locally by field investigators. For investigations requiring other record checks, reference interviews, and/or a Subject Interview, tasking is sent from the ISP simultaneously to 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 investigator that developed the information to another field office. Investigative reports are electronically submitted as the work is completed. When all reports have been received at the ISP, the case is reviewed for completeness, and then forwarded to the appropriate Central Adjudication Facility (CAF).

How long does it take to process a security clearance?

In April 2012 DISCO reported average end-to-end processing time of 99 days for the fastest 90% of defense contractor Top Secret clearances and 52 days for Secret clearances.

With some exceptions most federal agencies are completing the fastest 90% of all initial clearances (Secret and Top Secret) close to the average of 60 days as required by the 2004 Intelligence Reform and Terrorism Prevention Act (IRTPA). This average for the fastest 90% can include cases that take up to about 180 days. The remaining 10% can take from 6 months to over a year.

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

No. A new application with need to be submitted and a completely new investigation will need to be conducted and adjudicated.

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?

Compared to a few years ago, the vast majority of clearances are now being completed much faster than they previously were, but some clearances continue to take a long time. For these cases part of the answer involves the applicant and requires a better understanding of the process. There are three phases to clearance

processing: 1) application initiation, 2) investigation, and 3) adjudication. In the past most clearance delays occurred during the investigation phase. Due primarily to a significant increase in the number of investigators, the average time for investigations has been significantly reduced. Today most of the delays in getting a clearance occur in the application initiation phase and the adjudication phase. The problems that cause these delays are:

1. The applicant is not available for a Subject Interview
2. Missing or inaccurate data on security clearance application forms
3. Problems involving fingerprint submission
4. Serious security/suitability issues
5. "Queuing time"

Problem #1 occurs during the investigation phase and is usually due to the applicant being out of the country. If the applicant is in a war zone, the Subject Interview is usually conducted when the applicant returns to the United States. There can also be substantial delays when an applicant is in a location, such as Germany, Japan, Great Britain, or South Korea.

Problems #2 and #3 occur primarily at the application initiation phase and can result in an application being rejected by the CAF or ISP and returned to the requestor. About 10% to 12% of all clearance applications are rejected. This can result in delays of 30 to 60 days. Reviews of applications at the CAF and at the ISP 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 omissions are only discovered during the investigation phase where the case can also be delayed.

Problems #4 and #5 occur primarily at the adjudication phase and can result in much longer delays. Serious issues may require additional information or investigation. When a CAF requests additional information or investigations, it can delay a case for months. A certain amount of queuing time is necessary for efficient operations, but when there is a backlog of cases with major issues, queuing time becomes excessive.

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

1. Download a printable copy of the application form (Standard Form 86—SF86) from the OPM website. Complete the printed copy of the SF86, before attempting to complete the electronic (e-QIP) 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. Among other things, failure to list the organization that is sponsoring your clearance as you current employer will cause your application to be rejected.
3. Postal Zip Codes are critical. A wrong Zip Code can result in part of your investigation being sent to the wrong investigative office, and the case could languish for days before the error is noticed. Get Zip Codes at https://www.usps.com/zip4/.
4. Get a free credit report from 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, try to list neighbors. Avoid listing relatives in any section of the SF86, except Section 17—Marital Status and Section 18—Relatives.
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 and check the citizenship laws of the foreign county where you were born. If you have dual citizenship, you should indicate in the SF86 your willingness to renounce foreign citizenship.
7. If you have a foreign passport due to dual citizenship, arrange with the security office processing your clearance to either surrender or destroy the passport. Indicate in the "Optional Comments" field of the e-QIP version of the SF86 that you have either surrendered the passport to the appropriate security officer or destroyed it in his/her presence. Obtain a written receipt or a statement from the security officer regarding the disposition of your foreign passport. Do not contact any foreign official regarding the foreign 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 forms for release of medical information. If not, get a blank copy of their release and take it with you when you are interviewed by an investigator.
9. If you left a job under less than favorable circumstances, explain the situation in the "Optional Comments" field of section of Section 22 of your e-QIP, 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 and implemented in 2006. There are 13 guidelines covering such things as alcohol consumption, drug involvement, financial considerations, criminal conduct, etc. Each provides examples of 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, use the "Optional Comments" field and add contact information for a former coworker or second tier supervisor. For schools you should list former classmates 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), an Enhanced Subject Interview (ESI) is a regular part of the investigation. ESIs can also be required in an investigation for a Confidential or Secret clearance,

if a suitability/security issue is listed on your clearance application or surfaces during the investigation. A Special Interview (SPIN) can be required in any investigation, if a previously undisclosed suitability/security issue surfaces during an investigation after an ESI was conducted.

What will I be asked during a security clearance interview?

During a ESI, 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, susceptibility to blackmail, 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?

You must answer all questions on the clearance application form truthfully and completely, but you do not have to volunteer unfavorable information that is not related to any of the questions on the form. Many clearance denials for financial problems, drugs, alcohol, and criminal conduct also involve providing false information during the clearance process. Often the act of providing false information is more serious than the issues people try to hide. 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 a serious criminal offense and is very difficult to mitigate because of the recency of the offense.

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

1. Fingerprints not received with required timeframe of 14 days
2. Missing information on employment.
3. Missing information on references (education, employment, and/or character references)
4. Illegible Certification/Release forms
5. Certification/Release forms not meeting date requirements
6. Missing information on relatives
7. Missing Selective Service registration information
8. Incorrect date or place of birth (i.e. information on fingerprint card and SF86 don't match)
9. Missing financial information
10. Missing information on cohabitant
11. Missing information on spouse
12. Incorrect Certification/Release form number
13. Incorrect social security number

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

For DoD clearances only your security officer may inquire about the status of your security clearance application. This can be done 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 your security office, receive a security briefing, and required to sign a "Classified Information Non-disclosure Agreement," 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 many people these issues can be mitigated, if presented properly during a security interview or in response to a Letter of Intent to deny clearance.

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 unmitigated derogatory information, the adjudicator issues 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 LOI contains instructions on how to request a copy of the investigative file on which the decision to issue the LOI was based.

Industrial applicants (federal contractor personnel) can submit a written rebuttal to the SOR and request a hearing. If the applicant does not rebut the SOR, DoDCAF will deny the clearance. If the applicant rebuts the SOR without requesting a hearing, DoDCAF sends the applicant a File of Relevant Material (FORM) that will be presented to an Administrative Judge (AJ) for a clearance decision based on the written record. The applicant can submit a written response to the FORM, which will also be presented to the AJ. If the applicant requests a hearing, the applicant (with or without an attorney or personal representative) may present witnesses and other evidence at the hearing. The applicant may also cross-examine witnesses and challenge evidence presented by the DoDCAF Department Counsel (an attorney representing DoD). The AJ makes a written decision and a copy is sent to the applicant. DoDCAF is then directed to grant or deny the clearance in accordance with the AJ's decision. If the clearance is denied, the applicant is notified in writing and advised of their right to appeal the decision. It is possible that an adjudicator could grant the clearance after reviewing the applicant's response to the SOR, thus obviating the need to present the case to an AJ.

DoD civilian employees and military personnel can submit a written rebuttal to the SOR, but they are not entitled to a hearing. If the applicant does not rebut the SOR, DoDCAF will deny the clearance. If they submit a written rebuttal to the SOR, the adjudicator will decide to grant or deny the clearance in light of information submitted in the rebuttal. If a decision is made to deny a clearance, the applicant is notified in writing and advised of their right to appeal the decision.

Can I appeal a clearance denial or revocation?

Any applicant may appeal a clearance denial or revocation to the federal agency's three-member Personnel Security Appeals Board (PSAB). PSAB decisions are made by a majority vote.

Industrial applicants are limited to submitting a written appeal, but the PSAB will not consider any new evidence. The appeal must be based on procedural error(s) by the AJ. In industrial cases the DoD Department Counsel can appeal the favorable decision of an AJ. The PSAB issues a written decision addressing the material issues raised on appeal and a copy is sent to both parties. The PSAB can affirm, reverse, or remand a case to the original AJ with instructions for further review. If the original decision is reversed or affirmed, the decision of the PSAB is final.

DoD civilian employees and military personnel have the choice of submitting a written appeal with supporting documents directly to their PSAB or requesting a personal appearance before an AJ. In either case new evidence can be submitted. Those who choose to appear before an AJ are permitted to explain their case (with or without an attorney or personal representative), submit supporting documents, and present witnesses, but it is not a hearing and there is usually no opposing counsel. The AJ evaluates all the information and makes a written clearance recommendation to the applicant's PSAB. The PSAB is not required to follow the recommendation of the AJ. The PSAB notifies the applicant of their final decision and includes reasons for their decision.

Applicants who are denied a clearance with or without an appeal are barred from applying for a security clearance for a period of one year.

What is the EPSQ (Electronic Personnel Security Questionnaire)?

The EPSQ was the only electronic security clearance application used within the DoD until July 2005, when it was gradually replaced by e-QIP.

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 "Questionnaire for National Security Positions" (Standard Form 86—SF86). E-QIP became available in July 2005 and slowly replaced the EPSQ. E-QIP now accounts for over 95% of all clearance applications.

What is JPAS (Joint Personnel Adjudication System)?

JPAS is the official personnel security clearance database management system for DoD, including National Industrial Security Program (NISP) cleared contractors. This system is used for all types of personnel clearance actions, including initiating requests for clearance investigations. JPAS is managed by the Defense Manpower Data Center (DMDC). For more information, visit the DMDC website.

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 more than 90% of all clearance investigations over the past 35 years. Additionally, due to the transfer of the DoD personnel security investigations function from DSS to OPM on February 20, 2005, any requests for DSS investigations completed after February 20, 2005 should be sent to the OPM. DSS only maintains those personnel security investigations completed by DSS prior to the February 20, 2005 transfer.

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 (DSS)
Office of FOIA and Privacy
27130 Telegraph Rd.
Quantico, VA 22134

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 feel may help in searching for records pertaining to you

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 use for collateral security clearances, unless they are necessary to resolve serious credible derogatory information that cannot 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. Within DoD, polygraph screening exams used to determine initial eligibility for special assignment or special access are limited to two types of polygraph exams, and either one or both exams may be administered.

A Counterintelligence Polygraph is the most common type of polygraph exam. 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
- Terrorist Activities
- Deliberate damage of U.S. Government Information Systems
- Intentional compromise of U.S. Government Classified Information
- Secret contact with a foreign national or representative

A Lifestyle Polygraph asks the candidate questions concerning their 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 can also attempt to look for issues in a person's private life for which he or she might be susceptible to blackmail or coercion. DoD Lifestyle Polygraph exam questions cover the following topics.

- Involvement in a serious crime
- Personal involvement with illegal drugs during the last seven years
- Deliberate falsification of the security forms
- A Full Scope Polygraph exam is a combination of both the Counterintelligence and Lifestyle polygraphs

Types of Investigations

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

An NACLC is the type of investigation required for a Secret or Confidential clearance for military and contractor personnel. 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.

ANACI (Access National Agency Check with Inquiries)

An ANACI is an investigation required for a Secret or Confidential clearance for new federal employees. It is a combination of the National Agency Check with Inquiries (NACI) used for federal employment suitability and the NACLC. It includes all the components of an NACLC plus written inquires to past and present employers, schools, and references covering the past 5 years.

SSBI (Single Scope Background Investigation)

An SSBI is a more detailed investigation than the NACLC and is required for a Top Secret clearance, for Sensitive Compartmented Information (SCI) access, and for designated Special Access Programs (SAP) at the Secret level. It includes an NACLC, an Enhanced Subject Interview (ESI), interviews of former spouses; interviews of character, employment, neighborhood, and educational references; reviews of residence, 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.

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

An SSBI-PR includes an NACLC, ESI, 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 NACLC, ESI, 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.

Interval of Periodic Reinvestigations

People with security clearances must be routinely reinvestigated at set intervals based on the level of clearance they possess. A PR 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 NACLC every 10 years
- Confidential requires an NACLC every 15 years

In the near future the interval of PRs for Confidential and Secret clearance will change to 5 years. There is a plan to change the PR interval for Top Secret clearances to 1 year by December 2013.

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

A trustworthiness investigation is a DoD term used for a background investigation for a person who is nominated for non-critical sensitive or critical sensitive national security position that does not involve access to classified information. Non-critical sensitive positions require the same investigation and reinvestigation required for a Secret clearance and critical sensitive positions require the same investigation and reinvestigation required for a Top Secret clearance.

Suitability Investigation

Suitability investigations are conducted on all new federal employees, either immediately before or shortly after they are hired. They are also conducted on federal contractor personnel being considered for "Public

Trust" positions or a "Personal Identity Verification" (PIV) card required by Homeland Security Presidential Directive 12 (HSPD-12). Within DoD a PIV is called a Common Access Card (CAC).

When based on the submission of an SF86 (Questionnaire For National Security Positions) rather than an SF85P (Questionnaire For Public Trust Positions), some suitability investigations are used to determine eligibility for both a Public Trust position and a Secret clearance.

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 agencies. 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 federal agency or a cleared contractor. A company cannot sponsor itself for an FCL. The cleared contract or federal agency requests the FCL when a definite, classified procurement need has been established.

How does a cleared contractor sponsor a company for a FCL?

Sponsorship is in the form of a letter to the Facility Clearance Branch of the Defense Security Service, 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 DoD Security Agreement (DD Form 441)?

A DD Form 441 is required for an FCL. It is an agreement between the Government and the contractor. The the Government agrees to issue the FCL and inform the contractor of the security classification of information to which the contractor will have access, and the contractor agrees to abide by the security requirements set forth in the National Industrial Security Program Operating Manual (NISPOM).

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 federal 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 requirements of the NISPOM the entire time it is a NISP participant.

What is a DSS inspection/review?

A DSS review is a periodic visit to the contractor facility 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 position 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 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. The cleared contractor or federal 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 the Defense Security Service.

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 SAPFs?

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 such cases 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 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 job opportunities that don't require a clearance?

Candidates without clearances can search for jobs that do not require clearances at other internet-based career sites like Dice.com (for IT candidates), Rigzone.com (oil & gas professions), HealthCallings.com (healthcare professions), and eFinancialCareers.com (finance professions).

Security Clearance Processing

How can I better understand the course of events that have shaped the personnel security clearance process?

The history is fairly long and complicated. However, certain specific events give a clear understanding of how the security clearance process has evolved since 1972, and the difficulties the US Government has faced.

It's important to recognize that federal security clearance processing does not exist within a single monolithic structure with one agency conducting investigations and one agency making clearance decisions. There are dozens of federal agencies that process clearances. All agencies use the same basic procedures and standards for granting or denying clearances, but many agencies use their own resources to make clearance decisions. Most agencies use the Office of Personnel Management (OPM) as their Investigation Service Provider (ISP), but many agencies have statutory or delegated authority to use other ISPs or their own internal investigative personnel. Consequently there are significant differences in the time it takes to complete a security clearance.

About 87% of all Personnel Security Investigations (PSIs) are conducted on DoD personnel (federal employees, military, and contractors). The next largest are DHS (including its component agencies) at about 3% and DoE at about 1.2%. Each of the other agencies processes only a fraction of 1% of the 850,000 PSIs conducted each year. Because the DoD personnel security program dwarfs the combined size of all other federal agency programs, it's necessary to focus on DoD when discussing security clearance processing.

In 1972 the responsibility for Army, Navy, Air Force, and DoD contractor PSIs was transferred to the newly created Defense Investigative Service (DIS). A DoD Personnel Security Working Group (PSWG) published a report In April 1975 documenting the lack of standardization throughout the personnel security program. The PSWG reported that adjudications for collateral clearances were being performed in several thousand locations across DoD and repeated criticized the inconsistencies in adjudicative decisions. It also recommended that the number of different types of PSIs be reduced. Many of the PSWG's recommendations were implemented during the 1970's and 1980's, including the consolidation of several thousand adjudicative offices into 18 DoD Central Adjudication Facilities (CAFs). In December 1979 DoD Directive 5200.2, Personnel Security Program, and its

implementing regulation, DoD 5200.2-R were issue, and for the first time, most of the elements of personnel security were standardized throughout DoD. In 1981 the first formal Adjudicative Guidelines were established and incorporated into DoD 5200.2-R.

From its inception DIS was understaffed and had 48,000 pending cases (twice its optimum workload), many of which were overdue. From 1974 to 1985 its workload increased over 58% with 17% fewer investigators than the military had to do the job prior to 1972. A General Accounting Office (GAO) report in 1981 estimated that delays for initial clearances were costing the Government $920 million a year in lost productivity. That same year DIS imposed a moratorium on conducting Periodic Reinvestigations (PRs) for clearances involving access to Sensitive Compartmented Information (SCI), in order to deal with a large backlog of requests for initial investigations. In 1983 it resumed these PRs and also began conducting PRs for collateral Top Secret clearances. In 1985 the "Stillwell Commission" report recommendations resulted in additional funding for DIS and PRs for Secret clearances. DIS had about 850 field investigators at the time and began adding additional personnel. In 1991 it reached a high point of about 3,100 investigative personnel, including 2,400 field investigators. However, in anticipation of a reduction in security clearance requests because of the "peace dividend" resulting from the end of the Cold War, a hiring freeze was imposed. A 48% reduction-in-force occurred over the following 3 years and left DIS with about 1,600 investigative personnel of which 1,250 were field investigators.

During a second reform effort in the 1990's, the number of DoD CAFs was further reduced from 18 to 8, and the types of PSIs were reduced to 3. The Single Scope Background Investigation (SSBI) increased the amount of investigative work required for Top Secret clearances, and a "neighborhood investigation" component was added to the SSBI-PR. With only half the investigative personnel it previously had, DIS was forced to implement a quota system for PRs, restricting the number of requests defense agencies were allowed to submit. Nevertheless the backlog of cases at DIS began to grow. In 1998 the new investigative standards required by Executive Order 12968 were issued. The implementation of these standards immediately resulted in a "backlog" of 400,000 PRs, most of which were required by the new standards but not yet submitted to the Defense Security Service (DSS), which had changed its name from DIS 2 years earlier.

In 2000 DoD began shifting a large portion of security clearance investigations from DSS to the Office of Personnel Management (OPM). OPM was previously responsible for conducting federal employment suitability investigations (including those for DoD), as well as a relatively small number of security clearance investigations for other federal agencies. In 1996 OPM disestablished its Office of Federal Investigations and privatized the field portion of that organization through the creation of the US Investigations Services (USIS) under an Employee Stock Ownership Plan (ESOP). USIS was awarded a 3-year non-competitive contract to conduct investigations for OPM.

Foreshadowing the requirements of the Intelligence Reform and Terrorism Prevention Act (IRTPA), the 2004 Defense Authorization Bill directed DoD to begin submitting almost all of its security clearance investigations to OPM in early 2004, and DSS investigators began conducting those investigations under OPM control. According to a 2004 GAO report, DSS and OPM had a combined investigative staff of 4,200 government and contractor personnel. OPM estimated that about 8,000 were needed. The average turnaround time for an SSBI hit a high of about 396 days.

In December 2004 the IRTPA became law. It required that, to the extent possible, all executive branch security clearance investigations be conducted by one agency. It also required that 90% of all security clearances be completed in an average of 60 days by December 2009. In January 2005 GAO designated the DoD Personnel Security Program as a high-risk program. In March 2005 1,600 federal investigative personnel officially

transferred from DSS to OPM. By the end of 2005 the Federal Investigative Services Division of OPM increased its combined contractor and federal work force to about 8,000, including 6,500 field personnel. By 2008 OPM investigative staff reached a high of 9,421 personnel, but has declined somewhat since then. Unlike DSS, which was an appropriated fund activity, OPM conducts investigations on a fee-for-service basis and has the authority to set the prices it charges other Government agencies for the investigations they request. The combination of being paid for the investigations it conducted and using contract investigators to do the majority of the work afforded OPM the flexibility to rapidly adapt to changes in the number and type of investigations it conducted. Gradually the backlog of cases and the average turnaround time for investigations began to decline.

In early 2007 the Office of Management and Budget (OMB), the Office of the Director of National Intelligence (ODNI), OPM and DoD created a Joint Security and Suitability Reform Team (JSSRT) to completely revamp and unify the process. The JSSRT issued its initial report in April 2008 outlining a general framework for near and long term goals to modernize and streamline security clearance, employment suitability, and access to federally-controlled facilities and information systems government-wide. In December 2008 the JSSRT issue a progress report detailing the changes it initiated and planned to implement over an 18 month period. Some of these changes were implemented on schedule, some were delayed, modified, or partially implemented, and new changes were added. Full implementation of all the original or modified changes will probably not occur until 2014.

The most notable events that have occurred since 2008 are:

Aug 2009 Secure Web Fingerprint Transmission (SWFT), a web-enabled biometric system, became available to defense contractors to transmit electronic fingerprints to OPM for security clearance applicants. Federal contractors will be required to submit all fingerprints via SWFT by December 2013.

Apr 2010 The Case Adjudication Tracking System (CATS) became operational at all major DoD Central Adjudication Facilities. This enabled the electronic transfer of completed investigations from OPM and conversion of these files to a machine readable format. It resulted in reducing the transfer time by 50% and permitting electronic adjudication (eAdjudication) of about 25% of Secret clearance investigations.

Jul 2010 The Defense Central Index of Investigations (DCII) was transferred from DSS to the Defense Manpower Data Center (DMDC). This completed the transfer of DoD Personnel Security IT Systems from DSS to DMDC. Previously the Joint Personnel Adjudication System (JPAS), the Secure Web Fingerprint Transmission (SWFT), and the improved Investigative Records Repository (iIRR) were transferred from DSS to DMDC. These systems will eventually be integrated into the Defense Information Systems for Security (DISS) along with the Industrial Security Facility Database (ISFD) and Educational Network Registration and On-Line Learning (ENROL). DISS also provides Automated Records Check (ARC) and eAdjudication functionality and is the single point of entry for DoD personnel security.

Oct 2010 The Enhanced Subject Interview (ESI) replaced the Personal Subject Interview (PRSI) as a standard component of all Single Scope Background Investigations (SSBIs), Background Investigations (BIs), and Moderate Risk Background Investigations (MBIs). It also partially replaced the Special Interview (SPIN) required on investigations for Secret clearances when an interview of an applicant is needed to resolve unfavorable information.

Oct 2010 OPM eliminated the Limited Investigation (LI), the Periodic Reinvestigation—Residence (PRI-R), and the Public Trust Special Background Investigation (PTSBI), which had previously been used for Public Trust positions.

Feb 2011 The Government Accountability Office (GAO) reported removal of the Department of Defense (DOD) Personnel Security Program from its list of High Risk Programs, because of improvements to the program since it was first placed on the list in 2005.

Sep 2011 December 2010 version of the SF86 (Questionnaire for National Security Positions) was fully implemented.

Dec 2011 Title 5 Code of Federal Regulations Part 731 (5 CFR 731), "Suitability," was changed to require Periodic Reinvestigations (PRs) on all "covered" Public Trust positions at 5-year intervals. PRs were previously not required by 5 CFR 731.

Aug 2012 Six DoD Central Adjudication Facilities (CAFs) began consolidating into a single a CAF. The consolidation is expected to be completed by January 2013. By September 2013 the new DoDCAF is expected to expand its responsibilities to adjudicating federal employment suitability and Homeland Security Presidential Directive 12 credentialing determinations. The 3 other DoD CAFs (National Security Agency, Defense Intelligence Agency, and National Geospatial Intelligence Agency) are not included in the consolidation.

Overall the Government has met the IRTPA timeliness requirement to complete 90% of initial clearances in an average of 60 days, but major problems involving reciprocity of security clearances still exist and a single integrated database of all security clearances has not been created. OPM has significantly reduced the time it takes to conduct investigations, but the quality of investigations has declined and increased the time required to adjudicate problematic cases.

In 2013 the interval for Periodic Reinvestigations (PRs) for Confidential and Secret clearances will be shortened to 5 years, and in 2014 PRs for Top Secret clearances will be conducted annually. The scope of an investigation for a Top Secret clearance will change significantly. There will be a greater reliance on a combination of commercial and government database searches and a reduction in the number and type of interviews and record checks conducted by field investigators.