

SECURITY CLEARANCES 101 ANSWERS TO FREQUENTLY ASKED QUESTIONS

Get answers to frequently asked questions about U.S. Government security clearances, the National Industrial Security Program, and Department of Defense Personnel Security and Facility Security Programs. Learn more about security clearance processing timelines, how to fill out the SF-86, the criteria for obtaining a security clearance, and polygraph procedures in this comprehensive guide to the security clearance process.

Table of Contents

Section 1: The Security Clearance Explained	05
What is a security clearance?	05
What are the security clearance levels?	05
What is a collateral clearance?	05
What is a "special access authorization"?	05
How can I be granted Sensitive Compartmented Information access?	06
What is a Special Access Program?	06
Can you get an interim eligibility for access for SCI/SAP?	06
What is the DoD Central Adjudication Facility?	06
What is the Defense Office of Hearings and Appeals?	06
What type of information is requested on a security clearance application?	07
How long does a security clearance remain in effect?	07
When is a security clearance terminated?	07
Can a security clearance be reinstated after it has been terminated?	07
What is an interim security clearance?	08

Section 2: Getting a Security Clearance	
Can I obtain a security clearance on my own?	
Can non-U.S. citizens obtain security clearances?	

Section 3: Personnel Security Clearances (PCL)	09
What are the steps to getting a Personnel Clearance?	09
Who issues security clearances?	09
How much does it cost to get a Personnel Security Clearance?	09



Sec	tion 4: Security Clearance Process	10
000	How are security clearance investigations carried out?	10
	How long does it take to process a security clearance?	
	Will my clearance be granted faster because I previously held a security clearance?	
	Will my security clearance be granted faster if I have immediate family members	
	who have clearances?	_11
	Why does it take so long to get a security clearance?	_11
	What can I do to speed up the process of getting a security clearance?	. 12
	Who should I list as references on my security clearance application?	13
	Will I be interviewed by an investigator?	13
	What will I be asked during a security clearance interview?	. 13
	Should I reveal unfavorable information about myself on my security clearance application?	13
	What are the most common errors requiring correction before the security clearance	
	investigation is opened?	. 14
	How can I find out the status of my security clearance application?	
	How will I be informed when I am granted a security clearance?	. 14
	What types of things can prevent someone from receiving a security clearance?	
	What happens when a security clearance is denied?	
	Can I appeal a security clearance denial or revocation?	
	What is Electronic Questionnaire for Investigations Processing (e-QIP)?	
	What is eApp?	. 16
	What is Joint Personnel Adjudication System (JPAS)?	
	What is Defense Information Systems for Security (DISS)?	
	What is the Defense Counterintelligence and Security Agency (DCSA)?	
	What is Continuous Evaluation?	
	What is Continuous Vetting?	. 17
	What is Trusted Workforce 2.0?	
	How can I get a copy of my security clearance investigation?	. 17

Section 5: Polygraphs	19
What are polygraphs?	19
What are the differences between Counterintelligence, Lifestyle, and Full	
Scope Polygraphs?	19



Section 6: Types of Security Clearance Investigations _____

Tier 3 Investigation	20
Tier 3R Investigation	20
SSBI (Single Scope Background Investigation)	20
SSBI-PR (Single Scope Background Investigation—Periodic Reinvestigation)	20
PPR (Phased Periodic Reinvestigation)	20
Tier 5R Investigation	21
Cyber Vetting	21
Reimbursable Suitability Investigation (RSI)	21
Trustworthiness Investigation	21
Federal Employment Suitability Investigation	21
Federal Employment Fitness Investigation	21

Section 7: Facility Security Clearances	_ 22
What is the National Industrial Security Program (NISP)?	22
How does a company get a facility clearance (FCL)?	22
How does a cleared contractor sponsor a company for a FCL?	22
What is a DoD Security Agreement (DD Form 441)?	22
What is a Contract Security Classification Specification (DD Form 254), and how	
does it relate to a FCL?	22
What is a DCSA Industrial Security Representative (IS Rep)?	22
What is a DSS inspection/review?	23
Who has to be cleared in connection with a FCL?	23
What happens if a "controlling" officer cannot be cleared in connection with the FCL?	23
What is a Facility Security Officer (FSO)?	23
Does the FSO have to have a personnel clearance? What level?	23
What is an Insider Threat Program?	23
How does a company get a Top Secret FCL?	24
How much does it cost to get a FCL?	24
What is Foreign Ownership, Control or Influence (FOCI)?	24
What are SCIFs and SAPFs?	24
Who inspects SCIFs and SAPFs?	24

Section 8: Security Clearance Jobs _____ 25

Where can I search for jobs that require a security clearance?	25
If I don't have a security clearance, where can I find employers that might be able	
to sponsor me to receive one?	25



20

Section 1: The Security Clearance Explained

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 is used in Government record systems and by Government personnel security specialists. There are two types of clearances: <u>Personnel Security Clearances</u> (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 is a collateral clearance?

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

What is a "special access authorization"?

Access to classified national security information is based on an appropriate level of security clearance (Confidential, Secret, or Top Secret) and a "needto-know." Need-to-know can be either a formal or an informal determination. All classified national security 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 (SAPs), 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 needto-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?

In order to be considered for <u>SCI eligibility</u>, an applicant must first be nominated for an SCI billet, complete a Single Scope Background Investigation (SSBI), and be approved by the government agency that controls the information. Since SCI encompasses several categories of compartmented information, Central Adjudication Facilities (CAFs) grant eligibility for access to SCI, and 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 three 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 Special Access Program (SAP) is established to control access, distribution, and provide protection for sensitive classified information beyond that normally required. This is a high state of enforced need-to-know, and only a minimum number of cleared employees are given access.

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.

What is the DoD Central Adjudication Facility (DoD CAF)?

In summer 2011, all nine DoD Central Adjudication Facilities (CAFs) relocated to a new building on Fort Meade, MD. Between August 2012 and January 2013, six of these CAFs (Army CCF, DoN CAF, AFCAF, JCS CAF, WHS CAF, and DISCO/DOHA consolidated into one DoD CAF. The former CAFs were eventually reorganized into four divisions. The Industry Division (Division A) of DoD CAF consists of the former DISCO and DOHA staff adjudicators and support personnel. The other three CAFs (NSA, DIA, and NGA) remain separate entities.

What is the Defense Office of Hearings and Appeals (DOHA)?

The Defense Office of Hearings and Appeals is a component of the Defense Legal Services Agency. DOHA is comprised primarily of attorneys (Department Counsel), Administrative Judges, and administrative support personnel. DOHA previously had Personnel Security Specialists (staff adjudicators), but when DoD CAF was created, these personnel transferred to DoD CAF. In 2015 DOHA added Personnel Security Specialists to their staff to perform some functions related to HSPD-12 credentialing and federal employment suitability cases that are not done by DoD CAF. DOHA receives a few thousand of the most problematic cases each year from the Industry Division of DoD CAF, and about 1,500 of these cases are decided by their Administrative Judges. Most of these decision are based on evidence presented at a hearing requested by the applicant. DOHA Administrative Judges also preside over "Personal Appearances" (similar to hearings) of



clearance applicants appealing clearance denials or revocations by other divisions of DoD CAF.

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

The application form, Standard Form 86-SF-86 (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, certain types of mental health treatment, 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 seven years, some require 10 years, and others are not limited to any period of time. A PDF version of the SF-86 form is available at the OPM website; however, most applicants will use the Defense Counterintelligence and Security Agency web-based version called e-App.

How long does a security 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 <u>Periodic Reinvestigation</u> or <u>Continuous Vetting</u> requirements.

When is a security 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 gone out-of-date. Under such circumstances the clearance can be administratively restored.

Can a security clearance be reinstated after it has been terminated?

Yes. If a person previously had a clearance and the investigation has not gone out-of-date, 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-inservice of two years or more.

This can be done without the individual submitting a new SF-86; however, for clearances involving special access authorizations, a new SF-86 can be required if there has been a break-in-access of more than 60 days or if a polygraph examination is required.

Under certain circumstances, a clearance can be reinstated (recertified), if it is not more than two years out-of-date and a request for reinvestigation has been initiated.

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 and Top Secret clearances can be granted in as little as 30 days after the clearance granting authority receives a properly completed SF-86 and electronic fingerprints have been submitted. 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. The CAF is not required to provide a reason for the declination/withdrawal; however, it is possible to obtain this information using a <u>Privacy</u> <u>Act request</u>.

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.

Section 2: Getting a Security Clearance

Can I obtain a security clearance on my own?

No. You must be <u>sponsored by a cleared contractor</u> 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 sponsored 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 <u>U.S. citizenship per se does not</u> make a difference for security clearance eligibility.

Can non-U.S. citizens obtain security clearances?

No. You must be a U.S. citizen in order to be granted a security clearance; however, foreign nationals may be granted a Limited Access Authorization (LAA). LAAs are granted in those rare circumstances where a non-U.S. citizen possesses a unique or unusual skill or expertise that is urgently needed to support a specific U.S. Government requirement involving access to specified classified information (no higher than Secret), and a cleared or clearable U.S. citizen is not readily available.



Section 3: Personnel Security Clearances (PCL)

What are the steps to getting a Personnel Clearance?

For DoD clearances, a cleared contractor or DoD Government agency identifies an employee or employment candidate with a need to have access to classified information. Once identified, the contractor's Facility Security Officer (FSO) or the Government agency's Security Manager (SM) submits an investigation request through the Defense Information System for Security (DISS) and ensures that the individual completes an electronic security clearance application, eApp. The FSO then reviews, approves, and forwards the completed eApp to the Vetting Risk Operations Center (VROC) within DCSA for their approval, issuance of an interim clearance, and release to the Defense Vetting Directorate for investigation. For most federal employees and all military personnel, the Government agency SM reviews, approves, makes an interim clearance decision, and releases the completed eApp to DCSA. DCSA conducts an investigation and sends the results of the investigation to DoD CAF. DoD CAF either grants a clearance or issues a Letter of Intent to deny clearance with a Statement of Reasons. Clearances for other federal agencies are processed in essentially the same manner, but can involve a different Investigation Service Provider (ISP).

Who issues security clearances?

The Department of Defense Consolidated Adjudications Facility (DoD CAF) at Fort Meade, MD issues Personnel Clearances (PCL) for most DoD civilians, military personnel, and contractor personnel. 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, 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. Collateral 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 Personnel Security Clearance?

With very <u>limited exceptions</u>, there is no direct charge to individual applicants or to federal contractors for a PCL issued by DoD and most other federal agencies.



Section 4: Security Clearance Process

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. "Letter Inquiries" to employers, employment supervisors, etc. are also done centrally by an ISP. For investigations requiring other record checks, reference interviews, and a Subject Interview, tasking is sent from the ISP simultaneously to different field offices and assigned to individual investigators (either federal agents or contract investigators) in all locations involved. If the investigation develops information that requires additional 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?

The end-to-end processing time for a security clearance is primarily dependent on the type of clearance required, the federal agency involved, and the absence or presence of significant unfavorable information.

Under the 2004 Intelligence Reform and Terrorism Prevention Act (IRTPA), federal agencies are

required to complete the fastest 90% of all initial clearances (Secret and Top Secret) in an average of 60 days (not counting the 10 or 12 days required for case submission). This average for the fastest 90% can include completion times ranging from 30 to 180 days. The remaining 10% can take from six months to over a year.

For a few years, starting in about 2010, federal agencies were generally able to meet the IRTPA timeliness requirements. However, a number of events beginning in fall 2013 caused delays in both investigations and adjudications. The ability of Government agencies to meet the IRTPA requirements is largely dependent on funding. Although recent technological advances have reduced some of the manpower intensive aspects of investigations and streamlined other processes, new investigative requirements have added to the cost and time required for investigations. Many new changes are being implemented and will continue being implemented. It is not possible to know what impact they will have on timeliness for the foreseeable future.

Will my clearance be granted faster because I previously held a security clearance?

No. A new application will need to be submitted, and a completely new investigation will need to be conducted and adjudicated. If unfavorable information in a case was fully covered, and favorably adjudicated during the prior clearance processing, it could speed up the <u>adjudication</u> <u>phase</u> of a new clearance request.



Will my security clearance be granted faster if I have immediate family members who have clearances?

No.

Why does it take so long to get a security clearance?

Some security clearance determinations are made relatively quickly. Others may take a year or more. For these cases, part of the answer involves the applicant and requires a better understanding of the process. There are three <u>phases to clearance</u> <u>processing</u>: 1) application, 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 phase and the adjudication phase. The problems that cause these delays are:

- 1. <u>Missing or inaccurate data on security clearance</u> <u>application forms</u>
- 2. Problems involving <u>fingerprint submission</u>
- 3. Serious security/suitability issues
- 4. "Queuing time"

Problems #1 and #2 occur at the application phase and can result in an application being rejected by the CAF or ISP and returned to the requestor. About 5% 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 #3 and #4 occur primarily at the adjudication phase and can result in much longer delays. Serious issues may require additional information or investigation. Things like significant foreign contacts, multiple addresses, employment issues, or prior criminal conduct will require increased investigative time and require more time for an investigation to be completed. 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 security clearance?

- Download a fillable PDF copy of the application form (Standard Form 86—<u>SF-86</u>) from the OPM website. Complete the PDF copy of the SF-86 before attempting to complete the web-based (e-App) version online. You will save yourself a lot of time and frustration.
- 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, <u>failure</u> to list the organization that is sponsoring your <u>clearance</u> as your current employer may 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.
- 4. Get a free copy of your credit report from each of the three national credit reporting agencies at <u>www.annualcreditreport.com</u> and review them before completing an SF-86. Something you were unaware of may appear on one of the reports and cause delays.
- When entering the "Name of Person Who Knew You" in the Residence Section of the SF-86, try to list neighbors. Avoid listing relatives in any section of the SF-86, 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 <u>http://www.multiplecitizenship.com/documents/IS-01.pdf</u> and check the citizenship laws of the foreign county where you were born. This document is old and may be inaccurate, but it's a good initial reference document. If you have dual citizenship, you should indicate in the SF-86 your willingness to renounce foreign citizenship.
- 7. If you have been hospitalized for <u>specific</u> <u>medical conditions</u> or been diagnosed by a physician or healthcare professional with a mental health condition in the past seven years, contact the facility or physician and determine if they will accept standard government forms for release of information concerning your condition or treatment. If not, get a blank copy of a release acceptable to your clinician and take it with you when you are interviewed by an investigator.
- 8. If you left a job under less than favorable circumstances, explain the situation in the "Add

Optional Comments" field of section of Section 13 of your e-QIP, and give the name and/or position of the person who terminated you or asked you to quit.

9. Couch any unfavorable security and suitability information in terms directly applicable to the mitigating conditions listed in the Adjudicative Guidelines. On December 10, 2016 the Director of National Intelligence signed Security Executive Agent Directive (SEAD) 4, "National Security Adjudicative Guidelines." 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. There are also "General Criteria" listed at paragraph 2 of the Adjudicative Guidelines that are applicable to all of the 13 guidelines.

Who should I list as references on my security clearance application?

There are four 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 "Add 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 Secret Special Access Program (SAP), an <u>Enhanced Subject Interview</u> (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 after an ESI was conducted.

What will I be asked during a security clearance interview?

During an 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 my security 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 intentional omission of relevant information and/ or 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 an application or during a Subject Interview is a serious criminal offense and difficult to mitigate because of the recency of the offense.

What are the most common errors requiring correction before the security clearance 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 form and SF-86 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 security clearance application?

For DoD clearances only your security officer may inquire about the <u>status of your security clearance</u> <u>application</u>. This can be done by checking the Defense Information System for Security (DISS) or by telephoning the DoD Security Service Center at 888-282-7682. Applicants can check the status of their DCSA background investigation by telephoning 724-794-5612.

How will I be informed when I am granted a security clearance?

Normally, you will be contacted by your security office, receive a security briefing, and be required to sign a "Classified Information Non-disclosure Agreement," immediately prior to being granted access to classified information.

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

It is extremely difficult to mitigate the following security issues:

- <u>current unlawful use of or addiction to a</u> <u>controlled substance</u>
- determined to be mentally incompetent by a mental health professional approved by DoD
- criminal conviction resulting in incarceration for a period of one year or more
- discharge or dismissal from the Armed Forces under dishonorable conditions

Otherwise, the most common reasons for clearance denial are serious 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 National Security Adjudicative Guidelines 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 "<u>Statement of Reasons</u>" (SOR) detailing the issues that are the basis of the decision. Some agencies issue a Letter of Denial with an SOR, but it is essentially the same as an LOI. The LOI contains instructions on how to request a copy of the investigative file on which the decision to issue the LOI was based.

Federal contractor personnel can submit a written rebuttal to the SOR and request a hearing. If the applicant doesn't submit a rebuttal to the SOR, DoD CAF will deny the clearance. If the applicant rebuts the SOR without hearing, DOHA 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 DOHA Department Counsel (an attorney representing DoD). The AJ makes a written decision and a copy is sent to the applicant. DOHA then grants or denies 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 the DOHA Chief Department Counsel 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 doesn't rebut the SOR, DoD CAF will deny the clearance. If they submit a 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 of their right to appeal the decision, including a right to a "Personal Appearance" before a DOHA AJ.

Can I appeal a security 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.

Contractor applicants are limited to submitting a written appeal, but the DOHA 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 a DOHA 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. Although a Personal Appearance is very similar to a hearing; 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 Electronic Questionnaire for Investigations Processing (e-QIP)?

<u>E-QIP</u> 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 <u>Positions</u>" (Standard Form 86—SF-86). E-QIP became available in July 2005, but was replaced by eApp in 2018. E-QIP now accounts for over 95% of all clearance applications.

What is eApp?

In 2018, the Defense Information System Agency's National Background Investigation Services (NBIS) program office recently debuted eApp, the updated, more intuitive replacement to the old <u>eQIP</u> security clearance application for Secret (Tier 3) and Top Secret (Tier 5) investigations. Once eApp is fully implemented for all levels of applications eQIP will go away and be fully replaced by the new system.

What is Joint Personnel Adjudication System (JPAS)?

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).

What is Defense Information Systems for Security (DISS)?

In July 2016, DoD announced the integration of various personnel security (including JPAS), facility clearance, and training databases into the Defense Information Systems for Security (DISS), providing a single portal to request, conduct, and record personnel security actions.

What is the Defense Counterintelligence and Security Agency (DCSA)?

The Defense Counterintelligence and Security Agency (DCSA) was founded in 2019 and is the federal security agency responsible for the personnel and industrial security mission. Executive Order (EO) 13869 directed the transfer of the National Background Investigations Bureau (NBIB) from the Office of Personnel Management (OPM) to the Department of Defense (DoD).



What is Continuous Evaluation?

Continuous Evaluation (CE) was defined in EO 13467 and mandated in EO 12968, which was signed in 2008. The government's CE program is one aspect of current clearance reform efforts including Trusted Workforce 2.0. CE will evolve into the Continuous Vetting program.

What is Continuous Vetting?

Continuous Vetting was defined in EO 13764, and provides the context for reviewing the background of an individual continuously to ensure they meet the eligibility requirements for access to classified information. The Office of the Director of National Intelligence is establishing real-time review of an individual's background. Executive Correspondence entitled "Transforming Federal Personnel Vetting: Measures to Expedite Reform and Further Reduce the Federal Government's Background Investigation Inventory" was signed by the Director of National Intelligence and the Director of the Office of Personnel Management February 3, 2019. The EC lays out the minimum standards and criteria for Continuous Vetting, and it allows agencies in compliance with those criteria to move forward in eliminating Periodic Reviews (PR) in favor of the Continuous Vetting model..

What is Trusted Workforce 2.0?

In March of 2018 the Office of the Director of National Intelligence's National Counterintelligence and Security Center announced the Trusted Workforce 2.0 initiative. It was an effort to overhaul and improve the security clearance process, and update the policy framework that's been in place since the 1950s. The approach focuses on revamping and improving the security clearance policy framework, improving security clearance business processes, and modernizing the IT framework used in the personnel security process.

How can I get a copy of my security 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. Due to the transfer of the DoD personnel security investigations function from DSS to OPM on February 20, 2005, any requests for investigations completed after February 20, 2005 should be sent to the OPM. DSS no longer maintains personnel security investigations completed by DSS prior to the February 20, 2005 transfer. Those records are available from the Defense Counterintelligence and Security Agency (DCSA).

Submit Privacy Act Requests to:

Defense Counterintelligence and Security Agency Attn: FOIA/Privacy Office for Adjudications 600 10th Street Fort George G. Meade, MD 20755-5615

E-mail: dcsa.meade.dcsa-dvd.mbx.dodcaf-privacy-act@mail.mil

- 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.
- The address where you would like the records sent.

In addition, you must provide a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the following format:

If executed outside the United States: 'I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature).'

If executed within the United States, its territories, possessions, or commonwealths: 'I declare (or certify, verify, or state) under penalty of perjury

that the foregoing is true and correct. Executed on (date). (Signature).'

Photocopies of two different identity source documents. Examples of acceptable identity source documents are noted on the FOI/P Program Overview page.

For all other federal agencies contact the agency's Freedom of Information and Privacy Act office (or visit their website) for instructions.



information and tips at our Cleared **Recruiting Resource Center.**



What are polygraphs?

Polygraphs are instruments that measure physiological responses (respiration, pulse, blood pressure, and galvanic resistance) to stress. Among other purposes, 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 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. Polygraph screening exams are governed by <u>Security</u> <u>Executive Agent Directive 2</u> and <u>Intelligence</u> <u>Community Policy Guidance 704.6</u>. The exams used to determine 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
- Unauthorized disclosure or removal of classified information

A Lifestyle Polygraph asks the candidate questions concerning their personal life and conduct 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. Full Scope Polygraph exams are also known as Expanded Scope Polygraph exams.



Section 6: Types of Security Clearance Investigations

Tier 3 Investigation

This <u>new investigation was implemented in October</u> 2015 and replaced the <u>NACLC</u> (National Agency Check with Law and Credit) and the ANACI (Access National Agency Check with Inquiries) investigations. The Tier 3 investigation is required for a Secret or Confidential clearance for federal employees, military and contractor personnel. This investigation is basically the same as the ANACI investigation with a few enhancements. Information regarding the exact scope and period of coverage of the Tier 3 investigation is not publicly available.

Tier 3R Investigation

This new investigation was implemented in October 2015 and replaced the NACLC. The Tier 3R investigation is a <u>Periodic Reinvestigation</u> (PR) required for all Secret and Confidential clearance. Currently, PRs are required at 10-year intervals for Secret clearances and at 15-year intervals for Confidential clearances. Under Continuous Vetting, PRs will be replaced with Continuous Evaluation of cleared professionals.

SSBI (Single Scope Background Investigation)

The SSBI was <u>replaced by the Tier 5</u> investigation in September 2016. An SSBI is a more detailed investigation than the Tier 3 investigation 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 a National Agency Check, credit check, law enforcement record checks, 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. The Tier 5 investigation will be basically the same as the SSBI with a few enhancements. Information regarding the exact scope and period of coverage of the Tier 5 investigation is not publicly available.

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

The <u>SSBI-PR</u> is the standard PR for a Top Secret clearance and is conducted at 5-year intervals. An SSBI-PR includes a National Agency Check, credit check, law enforcement record checks, ESI, references interviews, and record reviews, covering at least the past five years.

PPR (Phased Periodic Reinvestigation)

The PPR is a less comprehensive and less expensive alternative to the SSBI-PR. It is also conducted at 5-year intervals. The investigation is similar to the SSBI-PR but involves 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.

Tier 5R Investigation

The Tier 5R investigation replaced both the SSBI-PR and the PPR in October 2016. Information regarding the exact scope and period of coverage of the Tier 5R investigation is not publicly available. With the implementation of Continuous Vetting, Top Secret clearance holders are evaluated on a continuous basis between investigative cycles.



Cyber Vetting

On May 12, 2016 the Office of the Director of National Intelligence (ODNI) issued <u>SEAD 5</u>, which authorizes federal agencies to collect, use, and retain publicly available social media information for Personnel Security Background Investigations and Adjudications. Except for some pilot projects that already exist, it will be several months to a year before the necessary policies, standards, training, and administrative requirements can be put in place for federal agencies to actually begin cyber vetting.

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. These investigations are adjudicated using the same standards used for security clearances.

Federal Employment Suitability Investigation

Suitability investigations are conducted on new "competitive service" federal employees, either immediately before or shortly after they are hired. The type of investigation depends on the risk level (Low Risk, Moderate Risk, or High Risk) of the position the employee or employment candidate will occupy. A favorable adjudication for any risk level automatically makes an applicant eligible for "Personal Identity Verification" (PIV) cards required by Homeland Security Presidential Directive 12 (HSPD-12). If the position also requires a national security clearance, a single investigation can be completed that fulfills both suitability and security clearance requirements.

Federal Employment Fitness Investigation

The requirements for a Fitness investigation are exactly the same as a Suitability investigation. The only difference is that Fitness investigations are conducted on new "excepted service" federal employees and these investigations can involve different adjudicative criteria and procedures than Suitability investigations. These investigations are also conduct on federal contractor personnel being considered for "Public Trust" positions or PIV cards required by HSPD-12. Within DoD a PIV is called a Common Access Card (CAC).



Section 7: Facility Security Clearances

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 31 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. There are over 13,500 contractor facilities that are cleared for access to classified information.

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

A company <u>must be sponsored for an FCL</u> 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. DSS has information at their website about the FCL process.

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 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 Forms 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 DCSA Industrial Security Representative (IS Rep)?

Once sponsored for a FCL, a contractor is assigned an IS Rep (a DCSA 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. IS Reps are Special Agents also known as <u>Industrial</u> <u>Security Specialists</u>.



What is a DCSA inspection/ review?

A DCSA review is a periodic visit to the contractor facility by a DCSA 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 DCSA 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), the Facility Security Officer (FSO), and the Insider Threat Program Senior Official (ITPSO) must be cleared. The positions of FSO and ITPSO can be filled by same person. Individuals who should be cleared in connection with a FCL are called Key Management Personnel (KMP). There are provisions for "excluding" some KMP from the requirement to obtain a PCL as part of the FCL; however, as a minimum the senior management official of the business entity and the FSO/ITPSO must be cleared.

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/ITPSO), 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 <u>has responsibility over the</u> <u>facility's security program</u>. During the time a facility is cleared, the FSO is the main POC for the DCSA 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.

What is an Insider Threat Program?

An insider threat program is a program that gathers, integrates, and reports "relevant and available information indicative of a potential or actual insider threat, consistent with <u>EO 13587</u>" and the November 2012 "<u>National Insider Threat Policy and</u> <u>Minimum Standards</u> for Executive Branch Insider Threat Programs." The requirement for this program was made applicable to cleared federal contractors with the May 2016 change to the "National Industrial Security Program Operating Manual" (<u>NISPOM</u>, DoDM 5220.22). Cleared contractors must



designate a "U.S. citizen employee, who is a senior official and cleared in connection with the FCL, to establish and execute an insider threat program."

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 government.

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

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

Who inspects SCIFs and SAPFs?

DCSA 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.



SCIF 101

Records are kept regarding who enters the secured room. Authorization and in most cases security clearance are required to enter.

No unauthorized cellphones, laptops or any other electronic devices are allowed inside.

Any classified information or documents discussed must remain in the SCIF, unless the information is being transported via a secure bag for storage in another SCIF.



Section 8: 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 <u>ClearanceJobs.com</u>.





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 security clearances at other internet-based job boards like Dice.com (for IT candidates). Many defense contractors also publish their own hiring pages for candidates 'willing to obtain security clearance.' In those cases, the employer is able to sponsor the candidate's security clearance for a specific job opening.

This document was compiled by William H. Henderson, retired federal investigator, and ClearanceJobs.com editors.



ClearanceJobs

A modern marketplace for career opportunities in national security



ClearanceJobs is your all-in-one <u>recruiting solution</u>. Much like a CRM, our unique system lets you work candidate leads through a funnel, converting cool passives to active candidates ready to make a move—to your company.

STRUGGLING TO HIRE? TRY SOURCING SERVICES



ClearanceJobs <u>Sourcing Services</u> matches you with a dedicated recruiting team that actively sources engaged cleared candidates, reviews their skills, and performs phone screens—all in a cost-efficient way, so you can make the best hires within your budget.

CLEARANCEJOBS CAREER EVENTS



Our <u>career events</u> are turnkey—scheduled, organized, and advertised to deliver prime cleared candidates for your inperson and virtual. Simply show up! With over 30 career fairs held each year throughout the country, ClearanceJobs Career Events is the leading producer of career fairs catering to security-cleared professionals.

Want to learn more?

Connect with a ClearanceJobs Recruiting Specialist today at **1.866.302.7264** or visit our website at <u>www.clearancejobs.com</u>

