

Introduction to the Federal Security Clearance Process

By R. Scott Oswald¹

- **What is a security clearance?**
- **When can I appeal to the MSPB?**
- **When can I file in federal court?**
- **What is a SOR?**
- **How should I respond to an SOR?**
- **What is the role of a Security Officer?**
- **When do I need an attorney?**

I. Overview of the Security Clearance Process

A security clearance is the determination by the federal government that a person is eligible for access to classified information or restricted physical areas. An individual may have access to classified information if they are at a place where such information is kept and the security measures in force do not prevent him or her from gaining knowledge of such information.²

The purpose of a security clearance review is to ascertain whether a federal government agency or department deems a candidate is able and willing to safeguard information relating to national security. Agencies inquire into a candidate's perceived loyalty, reliability, and trustworthiness by reviewing the candidate's history, relationships, and overall character. The basic levels of security clearance classification are Confidential, Secret, Top Secret and Top Secret/SCI.³

¹ R. Scott Oswald is the managing principal at *The Employment Law Group*® in Washington, D.C. (www.employmentlawgroup.com), where he litigates employment-related actions on behalf of employees, including federal employees and employees of federal contractors. The author gratefully acknowledges the assistance of Kellee Boulais Kruse, an associate at *The Employment Law Group*® and Andrew Moyer, a legal assistant at *The Employment Law Group*® in drafting the article.

² See, e.g., 32 C.F.R. § 154.3 (U.S. Department of Defense regulation defining the term "access").

³ Individual federal agencies' classifications may vary. For example, the U.S. Department of Energy designates their classifications, from highest level to lowest, as "Q," "Q(X)," "L," "L(X)," "Top Secret," or "Secret." 10 C.F.R. § 1016.3(A). Because of the thoroughness of the investigation, it often takes over two years to secure a "Q" clearance.

Only the federal government can grant a security clearance and the agency must initiate the process. The applicant must work for a federal agency or contractor, *i.e.*, the applicant's sponsor, and must conduct work that justifies granting him or her access to classified information, *i.e.*, in a sensitive position. A security clearance will generally remain in effect, subject to periodic reinvestigations, as long as the holder remains employed by the agency or cleared contractor and continues to require access to classified information and/or restricted physical areas.

Each agency issues its own security clearances, which are valid at the agency that grants the clearance and only for the specific purpose for which the agency grants the clearance. Each agency has established its own unique adjudication process. Some agencies such as the FBI, CIA, and NSA investigate a candidate's background using their own personnel. Other agencies such as the Department of Defense ("DOD")⁴, NASA, and Departments of Commerce and Agriculture rely on the Office of Personnel Management ("OPM") to investigate a candidate's background.

An individual's security clearance is not technically transferable. Rather, most agencies will rely upon a sister agency's adjudication of a security clearance so long as it is active and the agency has not received derogatory information calling into question the individual's suitability to have access to classified information.

The security clearance investigation can last as long as 18 months or more. If the agency grants the individual a security clearance, the agency will invite the individual to a security briefing. In the agency's security briefing, the agency's security officer will review the protocols that each grantee must follow to safeguard classified information, the scope of the information to which the grantee may have access, and the circumstances under which the grantee may view classified information.

If an employee's job description legitimately requires him or her to hold a security clearance, then that employee is no longer entitled to his or her job if the employee cannot secure or maintain a clearance.⁵

II. State of the Law Pre-1988

In 1960, President Eisenhower issued Executive Order 10865, titled "Safeguarding Classified Information Within Industry." Executive Order 10865 established an "Industrial Personnel Security Clearance Review Program," which the Department of Defense would administer. Executive Order 10865 also established a minimum standard of due process afforded to an employee when an agency denied or revoked his or her security clearance. The order offers the employee the following:

⁴ DOD issues over 80% of security clearances.

⁵ *See, e.g., Robinson v. Dep't of Homeland Sec.*, 498 F.3d 1361 (Fed. Cir. 2007).

- (1) A written statement of the reasons why his access authorization may be denied or revoked, which shall be as comprehensive and detailed as the national security permits.
- (2) A reasonable opportunity to reply in writing under oath or affirmation to the statement of reasons.
- (3) After he has filed under oath or affirmation a written reply to the statement of reasons, the form and sufficiency of which may be prescribed by regulations issued by the head of the department concerned, an opportunity to appear personally before the head of the department concerned or his designee, including, but not limited to, those officials named in section 8 of this order, for the purpose of supporting his eligibility for access authorization and to present evidence on his behalf.
- (4) A reasonable time to prepare for that appearance.
- (5) An opportunity to be represented by counsel.
- (6) An opportunity to cross-examine persons either orally or through written interrogatories in accordance with section 4 of matters not relating to the characterization in the statement of reasons of any organization or individual other than the applicant.
- (7) A written notice of the final decision in his case which, if adverse, shall specify whether the head of the department or his designee, including, but not limited to, those officials named in section 8 of this order, found for or against him with respect to each allegation in the statement of reasons.⁶

However, Executive Order 10865 did not clarify the role of the courts in reviewing the revocation or denial of a security clearance.

III. *Department of the Navy v. Egan*

In 1987, the U.S. Supreme Court heard the case of *Thomas E. Egan v. the U.S. Department of the Navy*.⁷ Egan had worked as a laborer in a submarine factory, which dismissed

⁶ SAFEGUARDING CLASSIFIED INFORMATION WITHIN INDUSTRY, 25 FR 1583 (1960).

⁷ *Dep't of Navy v. Egan*, 484 U.S. 518 (1988).

him after the Navy revoked his security clearance. Egan appealed the decision under 5 U.S.C. § 7513, which provides appeal rights, including a hearing, for certain federal government employees removed “for cause.”⁸ The full Merit Systems Protection Board (“MSPB”) sustained the Navy’s removal action. However, the Supreme Court held that the MSPB did not have authority to review the substance of a security clearance determination in their review of the merits of an adverse action.⁹ *Dep’t of Navy v. Egan*, 484 U.S. 518, 529 (1988). The Court limited the scope of the MSPB review to the following questions:

1. **Does the employee’s position require a security clearance?**
2. **Was the clearance denied or revoked?**
3. **Was the employee provided the procedural protections specified in 5 U.S.C. § 7513?**
4. **Was transfer to a nonsensitive position feasible?**

IV. Executive Order 12968 (1995)

President Clinton signed Executive Order 12968 in 1995. This order establishes a system to determine which employees should have access to classified information. The agencies grant access to classified information to employees whose backgrounds demonstrate “loyalty to the United States, strength of character, trustworthiness, honesty, reliability, discretion, and sound judgment.” Executive Order 12968 established uniform standards and procedures for evaluating applicants, which have been recently updated. See Section VII below.

V. Executive Order 13467 (2008)

Executive Order 13467 (“Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information”), signed on June 30, 2008, created the federal government’s unified security clearance structure. It designated the OPM as the government’s “Suitability Executive Agent,” with the authority to conduct federal employee suitability investigations and make determinations regarding “logical and physical access” to federal facilities and information systems.

In addition, the Executive Order created a “Suitability and Security Clearance Performance Accountability Council,” chaired by the Office of Management and Budget’s (“OMB”) Deputy Director for Management and reporting directly to the President. The

⁸ The regulation states, “Under regulations prescribed by the Office of Personnel Management, an agency may take an action covered by this subchapter against an employee only for such cause as will promote the efficiency of the service. 5 U.S.C.A. § 7513(a).”

⁹ Adverse actions include removal, suspension for more than 14 days, a reduction in grade or pay, or a furlough of 30 days or less. 5 U.S.C. § 7512.

Executive Order grants the Council the: (1) authority over the information systems used for security clearance processing, and (2) authority to issue policies ensuring the uniformity of suitability and security processes, or “aligned systems” as described in Section 2.1 of the Executive Order.

The Executive Order authorizes the federal government to continuously evaluate personnel who hold security clearances with the use of new commercial and government databases. Continuous evaluation involves automated reviews:

- Once every year for Top Secret clearance holders; and
- Once every five years for Secret or Confidential clearance holders.

Finally, the Executive Order designates the Director of National Intelligence (“DNI”) as the “Security Executive Agent,” with unilateral authority over security and public trust clearance processing. The DNI’s responsibilities include: (1) developing federal government-wide policies on security clearance and sensitive position investigations and adjudication, (2) deciding who will perform the investigations, and 3) deciding who will adjudicate the investigations and issue the clearances.

Pursuant to the Executive Order, the adjudicating party must determine that the applicant is:

- (i) suitable for Government employment;
 - (ii) eligible for logical and physical access;
 - (iii) eligible for access to classified information;
 - (iv) eligible to hold a sensitive position;
- or
- (v) fit to perform work for or on behalf of the Government as a contractor employee.¹⁰

VI. *Conyers and Northover*

The MSPB’s decisions in *Conyers* and *Northover* upheld the rights of employees who occupied sensitive positions which did not require security clearances or access to classified information and granted these employees a narrow pathway of reviewability outside of the agency’s review process.

In December 2010, the MSPB issued decisions in Appellants Devon Haughton Northover’s and Rhonda K. Conyers’s appeals against the U.S. Department of Defense.¹¹

¹⁰ Executive Order 13467, Sec. 1.3(a).

¹¹ *Northover v. Dep’t of Def.*, AT-0752-10-0184-I-1 (M.S.P.B. Dec. 22, 2010); *Conyers v. Dep’t of Def.*, CH-0752-09-0925-I-1 (M.S.P.B. Dec. 22, 2010).

Conyers was appealing her indefinite suspension and Northover was appealing his reduction in grade, both adverse actions appealable to the MSPB.¹² DOD had suspended Conyers because the agency had denied her “eligibility for access to sensitive or classified information.” It had revoked Northover’s “eligibility for access to classified information and/or occupancy of a sensitive position.”

During the course of the litigation, the parties stipulated: (1) That Conyers’s and Northover’s positions did not require them to hold a confidential, secret, or top secret clearance, and (2) That Conyers’s and Northover’s positions did not require that they have access to classified information.

In light of these stipulations, the MSPB held that *Egan* did not limit the MSPB’s statutory authority to review Conyers’s indefinite suspension or Northover’s reduction in grade. Further, the MSPB interpreted *Egan* as limiting the MSPB’s review of an otherwise appealable action – such as an indefinite suspension or a reduction in grade – only if the action the action **is based** on the denial, revocation, or suspension of a security clearance.

VII. Guidelines for Security Clearance Decisions

The adjudicative process for a security clearance is “an examination of a sufficient period of a person’s life to make an affirmative determination that the person is an acceptable security risk.”¹³ The adjudicative guidelines, consistent with Executive Order 12968, are as follows:

- A. **Allegiance to the United States:** An individual must be of unquestioned allegiance to the United States. The willingness to safeguard classified information is in doubt if there is any reason to suspect an individual’s allegiance to the United States.
- B. **Foreign Influence:** Foreign contacts and interests may be a security concern if the individual has divided loyalties or foreign financial interests, may be manipulated or induced to help a foreign person, group, organization, or government in a way that is not in U.S. interests, or is vulnerable to pressure or coercion by any foreign interest. Adjudication under this Guideline can and should consider the identity of the foreign country in which the foreign contact or interest is located, including, but not limited to such considerations as whether the foreign country is known to target United States citizens to obtain protected information and/or is associated with a risk of terrorism.

¹² 5 U.S.C. § 7512.

¹³ “Revised Adjudicative Guidelines for Determining Eligibility for Access to Classified Information,” December 29, 2005.

- C. **Foreign Preference**: When an individual acts in such a way as to indicate a preference for a foreign country over the United States, then he or she may be prone to provide information or make decisions that are harmful to the interests of the United States.¹⁴
- D. **Sexual Behavior**: Sexual behavior that involves a criminal offense, indicates a personality or emotional disorder, reflects lack of judgment or discretion, or which may subject the individual to undue influence or coercion, exploitation, or duress can raise questions about an individual's reliability, trustworthiness and ability to protect classified information. No adverse inference concerning the standards in this Guideline may be raised solely on the basis of the sexual orientation of the individual.
- E. **Personal Conduct**: Conduct involving questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations can raise questions about an individual's reliability, trustworthiness and ability to protect classified information. Of special interest is any failure to provide truthful and candid answers during the security clearance process or any other failure to cooperate with the security clearance process.
- F. **Financial Considerations**: Failure or inability to live within one's means, satisfy debts, and meet financial obligations may indicate poor self-control, lack of judgment, or unwillingness to abide by rules and regulations, all of which can raise questions about an individual's reliability, trustworthiness and ability to protect classified information. An individual who is financially overextended is at risk of having to engage in illegal acts to generate funds. Compulsive gambling is a concern as it may lead to financial crimes including espionage. Affluence that cannot be explained by known sources of income is also a security concern. It may indicate proceeds from financially profitable criminal acts.
- G. **Alcohol Consumption**: Excessive alcohol consumption often leads to the exercise of questionable judgment or the failure to control impulses, and can raise questions about an individual's reliability and trustworthiness.
- H. **Drug Involvement**: Use of an illegal drug or misuse of a prescription drug can raise questions about an individual's reliability and trustworthiness, both because it may impair judgment and because it raises questions about a person's ability or willingness to comply with laws, rules, and regulations.
- I. **Psychological Conditions**: Certain emotional, mental, and personality conditions can impair judgment, reliability, or trustworthiness. A formal diagnosis of a disorder is not required for there to be a concern under this guideline. A duly qualified mental health professional (*e.g.*, clinical psychologist or psychiatrist) employed by, or acceptable to and approved by the U.S. Government, should be consulted when evaluating potentially disqualifying and mitigating information under this guideline. No negative inference

¹⁴ Under this guideline, possession of a foreign passport is not a disqualifying condition for a Top Secret/SCI clearance, although failing to report the possession of a foreign passport is.

concerning the standards in this Guideline may be raised solely on the basis of seeking mental health counseling.

- J. **Criminal Conduct**: Criminal activity creates doubt about a person's judgment, reliability, and trustworthiness. By its very nature, it calls into question a person's ability or willingness to comply with laws, rules and regulations.
- K. **Handling Protected Information**: Deliberate or negligent failure to comply with rules and regulations for protecting classified or other sensitive information raises doubt about an individual's trustworthiness, judgment, reliability, or willingness and ability to safeguard such information, and is a serious security concern.
- L. **Outside Activities**: Involvement in certain types of outside employment or activities is of security concern if it poses a conflict of interest with an individual's security responsibilities and could create an increased risk of unauthorized disclosure of classified information.¹⁵
- M. **Use of Information Technology Systems**: Noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual's reliability and trustworthiness, calling into question the willingness or ability to properly protect sensitive systems, networks, and information. Information Technology Systems include all related computer hardware, software, firmware, and data used for the communication, transmission, processing, manipulation, storage, or protection of information.

The adjudicator is to assign each guideline an equal level of importance and may look at information unrelated to the guidelines as well in examining and investigating the applicant as a "whole person." The adjudicator is to resolve any doubts "in favor of national security," *i.e.*, against the applicant. In evaluating whether or not an applicant's conduct is relevant, the adjudicator must consider:

- 1) The nature, extent, and seriousness of the conduct;
- 2) The circumstances surrounding the conduct, to include knowledgeable participation;
- 3) The frequency and recency of the conduct;
- 4) The extent to which participation is voluntary;
- 5) The presence or absence of rehabilitation or other permanent behavioral changes;
- 6) The motivation for the conduct;
- 7) The potential for pressure, coercion, exploitation, or duress; and

¹⁵ These activities include any employment or service, whether compensated or volunteer, with the government of a foreign country; any foreign national, organization, or other entity; a representative of any foreign interest; or any foreign, domestic, or international organization or person engaged in analysis, discussion, or publication of material on intelligence, defense, foreign affairs, or protected technology.

- 8) The likelihood of continuation or recurrence.¹⁶

Further, when the adjudicator learns information about the applicant that presents a security concern, the adjudicator must consider whether or not the applicant:

- 1) Voluntarily reported the information;
- 2) Was truthful and complete in responding to questions;
- 3) Sought assistance and followed professional guidance, where appropriate;
- 4) Resolved or appears likely to favorably resolve the security concern;
- 5) Has demonstrated positive changes in behavior and employment; and
- 6) Should have his or her access temporarily suspended pending final adjudication of the information.¹⁷

VIII. Denial or Revocation of Clearance

A candidate who is denied a security clearance will be notified of the reason for that decision and will have an opportunity to file an appeal.¹⁸ Each agency has its own appeal process. This section contains examples of the processes used by several departments and agencies who issue the vast majority of security clearances.

1. Department of Defense Appeals Process

The Department of Defense Office of Hearings and Appeals (“DOHA”) processes security clearance denials for Department of Defense (“DOD”) components.¹⁹ DOD federal employees may not be terminated from their job solely for denial of a clearance until the adjudication process is complete. However, it is very common for such an employee to be placed on 30 days administrative leave with pay, followed by an indefinite period of administrative leave without pay until the matter is adjudicated.

¹⁶ *Id.*

¹⁷ *Id.*

¹⁸ Without explicit authorization from either the President or Congress, an agency may not deprive an agency employee or government contractor employee of his or her position, in a proceeding in which he or she was not afforded safeguards of confrontation and cross-examination. *Greene v. McElroy*, 360 U.S. 474 (1959).

¹⁹ DOD Components include the Office of the Secretary of Defense; the Military Departments; Chairman of the Joint Chiefs of Staff; Directors of Defense Agencies and the Unified and Specified Commands. 32 C.F.R. § 154.3(f).

Applicants denied a security clearance receive a Statement of Reasons (“SOR”) from the government, which may be rebutted by submitting a rebuttal to DOHA within 20 days.²⁰ The rebuttal must admit or deny every item in the SOR. If the applicant admits to an item in the SOR, he or she should provide extenuating or mitigating information.²¹

Upon receipt of the SOR rebuttal, DOHA sends the applicant a File of Relevant Materials (“FORM”). The applicant has 30 days from receipt of the FORM to submit a written response to the FORM. If a review of the rebuttal to the SOR and/or response to the FORM determines that allegations are unfounded, or evidence is insufficient for further processing, the DOHA will withdraw the SOR and grant or continue the clearance.

If the DOHA does not withdraw the SOR, the applicant may request a hearing before an Administrative Judge (“AJ”). If the applicant requests a hearing, the AJ will provide notice at least 15 days in advance of the time and place of the hearing. The hearing will be held at a location within a major city near the applicant’s place of employment or residence. The DOHA attorney and applicant may request that the opposing party provide advance information about witnesses to appear and evidence to be presented. The applicant must appear at the hearing in person with or without an attorney or other representation. Hearings are generally open, except when the applicant requests that it be closed or when the AJ determines that there is good cause to close the proceeding. Each party may cross-examine witnesses during the hearing, and the AJ will keep a verbatim transcript of the proceeding.

Following a hearing, the AJ will issue a written decision on the granting of a security clearance and the veracity of the allegations within the SOR. The AJ’s decision can be appealed to the DOHA Appeal Board within 15 days. The applicant may submit an appeal brief, but Appeal Board will not consider new evidence. Therefore, appeal must be based on an error made by the AJ. In a majority of cases, the DOHA Appeal Board’s decision is final. The DOHA Appeal Board may affirm or reverse any portion of the AJ’s findings, and may remand the case for further proceedings before the AJ. The DOHA Appeal Board affirms a vast majority of security clearance denials.

Once a security clearance has been denied or revoked through this process, the applicant is barred from reapplying for a clearance for a period of one year from the date of the initial adverse clearance decision. Denied or revoked applicants do not have a right to appeal security clearance denials or revocations in the federal or state courts.

2. Department of Energy Appeals Process

The Department of Energy (“DOE”) also has an Office of Hearings and Appeals, which it describes as its “quasi-judicial arm.” Applicants may ask the DOE OHA to convene an Appeal Panel if their security clearance is denied or revoked. The Appeal Panel consists of three

²⁰ The DOHA may grant an extension with good cause.

²¹ See Section V below for common examples of mitigating information.

members, each of whom are DOE Headquarters employees, U.S. citizens, and DOE “Q” clearance holders.²² DOE’s Deputy Chief for Operations, Office of Health, Safety and Security, serves as a permanent member of the Appeal Panel and as the Appeal Panel Chairman. The second member of the Appeal Panel is a DOE attorney designated by the General Counsel. The head of the DOE Headquarters element under whom the applicant works may designate an employee to act as the third member on the Appeal Panel; otherwise, the third member will be designated by the Chairman. Only one member of the Appeal Panel will be from the security field.²³

The Appeal Panel may initiate an investigation of any statement or material contained in the request for an Appeal Panel review and use any relevant facts obtained by such investigation in the conduct of the final decision process. The Appeal Panel may solicit and accept submissions from either the applicant or DOE officials that are relevant to the final decision process and may establish appropriate time frames to allow for such submissions. The Appeal Panel may also consider any other source of information that will advance the final decision process, provided that both parties are afforded an opportunity to respond to all third party submissions. All information obtained by the Appeal Panel becomes part of the administrative record.²⁴

Within 45 work days of the closing of the administrative record, the Appeal Panel must render a final written decision in the case based on an evaluation of the administrative record, findings as to each of the allegations contained in the notification letter, and any new evidence that may have been submitted. If a majority of the Appeal Panel members determine that it will not endanger the common defense and security and will be clearly consistent with the national interest, the Deputy Chief for Operations, Office of Health, Safety and Security, will grant or reinstate access authorization for the individual. The Appeal Panel written decision shall be made a part of the administrative record.²⁵

3. Department of Homeland Security Appeals Process

The Department of Homeland Security (DHS), which includes agencies such as the U.S. Secret Service, presents employees with a Notice of Review when the appeal a revocation or denial of a security clearance. Employees or contractors appealing a security decision by the DHS or one of its agencies go before a Security Appeals Board. The DHS Office of the Chief Security Officer (OSCO) has the responsibility of convening the Security Appeals Board.²⁶

²² “Q” is DOE’s highest security clearance classification. *See* n.2, *supra*.

²³ 10 C.F.R. § 710.29(b).

²⁴ 10 C.F.R. § 710.29(e).

²⁵ 10 C.F.R. § 710.29(f).

²⁶ Instruction for the Office of the Chief Security Officer, dated September 3, 2008

4. Department of Justice Appeals Process

When the Department of Justice or one of its agencies, including the Federal Bureau of Investigation (FBI) or the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) denies or revokes a security clearance, it must do the following:

- (1) [Provide the applicant] with a comprehensive and detailed written explanation of the basis for that decision as the national security interests of the United States and other applicable law permit and informed of their right to be represented by counsel or other representative at their own expense;
- (2) [Permit the applicant] 30 days from the date of the written explanation to request any documents, records, or reports including the entire investigative file upon which a denial or revocation is based; and
- (3) [Provide the applicant] copies of documents requested pursuant to this paragraph (a) within 30 days of the request to the extent such documents would be provided if requested under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act of 1974 (5 U.S.C. 552a), and as the national security interests and other applicable law permit.²⁷

The applicant then files a written reply and requests review of the determination “within 30 days after written notification of the determination or receipt of the copies of the documents requested pursuant to this subpart, whichever is later.” The applicant then receives:

- (1) Written notice of and reasons for the results of the review;
- (2) The identity of the deciding authority; and
- (3) Written notice of the right to appeal.²⁸

Within 30 days of receipt of this information, the applicant or employee may appeal that determination in writing to the Department of Justice’s Access Review Committee (“ARC”), established under 28 C.F.R § 17.15. The applicant or employee may request an opportunity to

²⁷ 28 C.F.R. § 17.47(a).

²⁸ 28 C.F.R. § 17.47(b) and (c).

appear personally, with an attorney or other representation of his or her choice, before the ARC and to present relevant documents, materials, and information.²⁹

The ARC consists of the Deputy Attorney General or a designee, the Assistant Attorney General for National Security or a designee, and the Assistant Attorney General for Administration or a designee. The Attorney General must approve any designations.³⁰ The ARC must issue its decision “as expeditiously as possible.”³¹ The ARC's decision is final unless the Attorney General requests a recommendation from the ARC and “personally exercises appeal authority.”³²

5. Central Intelligence Agency Appeal Process

When the Central Intelligence Agency (CIA) denies or revokes a security clearance, the applicant is:

- (1) Provided as comprehensive and detailed a written explanation of the basis for that determination as the national security interests of the United States and other applicable law permit.
- (2) Informed in this written explanation of their right to be represented by counsel or other representative at their own expense; to request any documents, records or reports upon which a denial or revocation is based; and, to request the entire investigative file as permitted by the national security and other applicable law.
- (3) Provided within 30 days, upon request and to the extent the documents would be provided if requested under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act (5 U.S.C. 552a), as applicable, any documents, records and reports upon which a denial or revocation is based.
- (4) Provided an opportunity to reply in writing to request a review of the determination within 45 days of receipt of the relevant documentation.

²⁹ 28 C.F.R. § 17.47(d) and (e).

³⁰ 28 C.F.R § 17.15(b).

³¹ 28 C.F.R. § 17.47(f).

³² 28 C.F.R § 17.15(a).

(5) Provided written notice of and reasons for the results of the review, the identity of the deciding authority in accordance with operational requirements, and written notice of the right to appeal.

(6) Provided an opportunity to appeal in writing to a high level panel, appointed by the SOIC³³, which shall be comprised of at least three members, two of whom shall be selected from outside the security field. Decisions of the panel shall be in writing, and final, except when the SOIC chooses to exercise the appeal authority personally, based on a recommendation from the panel, and provided to the individual.

(7) Provided an opportunity to appear personally and to present relevant documents, materials and information at some point in the process before an adjudicative or other authority, other than the investigating entity, as determined by the SOIC. A written summary or recording of such appearance shall be made part of the applicant's or employee's security record, unless such appearance occurs in the presence of the appeals panel described in subsection a.(6) of this section³⁴, in which case the written decision of the panel shall be made part of the applicant's or employee's security record.³⁵

This process may take up to five years, and the deciding officials will only consider new evidence directly related to the events that formed the basis of its initial decision. It will not consider any mitigating events that occurred after the initial denial.

6. National Aeronautics and Space Administration Appeals Process

In the event that the National Aeronautics and Space Administration (NASA) denies or revokes a security clearance, it follows the process laid out in its Directive 201.10 "Denial or Revocation of Security Clearance."

If the Senior Adjudicator reviewing the decision reaches an unfavorable outcome, he or she will forward a documented proposal to deny or revoke a clearance to the Center Chief of Security (CCS). If the CCS disagrees with the decision, he or she may remand the decision back

³³ "Senior Official of the Intelligence Community"

³⁴ Refer to paragraph 6 above.

³⁵ Director of Central Intelligence Directive 6/4 ANNEX D: Appeals Procedures -- Denial or Revocation of Access

to the Senior Adjudicator, “with specific, written recommendations for areas of expansion or clarification.” However, if the CCS concurs with the recommendation, he or she will notify the applicant in writing.

The applicant may request a review of the decision and/or provide new information for consideration. The CCS must conduct another review, considering any new information provided. However, if after conducting this review, the CCS continues to recommend denial or revocation, the complete case file and the CCS recommendation go to the Director of Security Management Office (DSMO). After reviewing the file and CCS recommendation, the DSMO may do one of the following:

- (1) Remand the case to the CCS for further work; or
- (2) Make a favorable adjudication of the information; or
- (3) Provide written notice to the subject of the denial or the revocation of the security clearance.

If the DSMO provides notice of denial or revocation and the applicant requests appeal by the Security Adjudication Review Panel (SARP), the NASA Administrator will appoint the SARP. The SARP is made up of three NASA employees “who have demonstrated reliability and objectivity in their official duties.” SARP members “must have been the subjects of a favorable SSBI³⁶, and only one of the panel members may be a security professional.” If the Administrator believes that it would be inappropriate to use a NASA security professional, an outside security expert may sit on the SARP.

Prior to finalizing their determination, a SARP panel member or the DSMO may refer the SARP proposed decision to the Administrator for an additional level of review. If the SARP does not request this review, its decision is final. If the SARP does request the Administrator’s review, the Administrator's decision is final.

IX. Practical Tips

1. Before submitting your application

An applicant may believe that if he or she forgets to include information in the application, he or she may simply explain the error at a later point, perhaps during their interview with the investigator. However, the investigator will likely view this omission as a deliberate attempt to conceal damaging information, which will often lead to a denial. Therefore, use care to disclose all information in the application, including potentially damaging information. If you realize that you have submitted an incomplete application, **volunteer to supplement the application before the interviewer asks you about the omission.** Once the interviewer asks about the omission, you have no longer voluntarily provided the information which is generally considered to be a mitigating factor in a security clearance decision.

³⁶ Single Scope Background Investigation

2. After your security clearance is granted

An individual who holds a security clearance has an affirmative responsibility to inform the agency of any event that would affect his or her eligibility to maintain their clearance, *e.g.*, a criminal conviction. An agency is less likely to revoke a security clearance if the individual voluntarily discloses this information. Look to the security clearance guidelines³⁷ for potentially disqualifying events.

3. If your security clearance is denied

If your security clearance is denied, you will have the opportunity to appeal the decision as explained in Section IV above. After reviewing the SOR or equivalent document setting forth the reasons for the denial, collect the necessary evidence to correct any mistakes in the document. In the event that these issues are not mistakes, collect evidence to prove mitigating factors. Some examples of mitigating factors include:

- Has a great deal of time elapsed between the conduct in question and the application for a security clearance?
- Did the applicant voluntarily report the conduct in question?
- Did the applicant make good faith efforts to promptly correct any misstatements or omissions in the application?
- Was the misstatement or omission based on good faith reliance on improper or inadequate advice by agency personnel or legal counsel?
- Has the applicant voluntarily taken steps to change unfavorable behavior (*e.g.*, substance abuse, gambling addiction), such as obtaining professional counseling? Are there clear indications that the behavior is changing or under control?
- Was the conduct in question unintentional or inadvertent and was followed by a prompt, good faith effort to correct the situation?
- In the case that the applicant was associated with a questionable organization, was the applicant aware of the organization's unlawful aims? Did the applicant sever ties upon learning of the organization's unlawful aims?
- In the case of contact with foreign citizens, was the contact in question casual and infrequent? Was the contact approved by a U.S. security agency?

³⁷ Section III, *supra*

- In the case of dual citizenship, is this status based solely on a parent's citizenship or birth in a foreign country? Has the applicant expressed an interest in renouncing the dual citizenship?
- In the case of questionable sexual conduct, was the behavior in question private, consensual, legal, and discreet?
- In the case of unfavorable financial circumstances, did the problems occur due to factors beyond the applicant's control, such as loss of employment, a business downturn, unexpected medical emergency, or a death, divorce or separation? If so, did the applicant react responsibly given the circumstances?
- In the case of substantial debt, did the applicant make good faith efforts to repay overdue creditors or otherwise resolve the debts?
- In the case of unexplained affluence, can the applicant prove that the money came from a legal source of income?
- In the case of illegal drug use, has the applicant demonstrated any or all of the following behaviors:
 - disassociation from drug-using associates and contacts;
 - changing or avoiding the environment where drugs were used;
 - an appropriate period of abstinence;
 - a signed statement of intent with automatic revocation of clearance for any violation;
- In the case of abuse of prescription drugs, did the behavior in question occur after a period of severe or prolonged illness during which a doctor had prescribed the drugs? If so, has the applicant since ceased the abuse?
- In the case of a psychological condition, is the condition in question readily controllable with treatment and is the applicant participating in such treatment? Has the condition been resolved?
- In the case of a past period of emotional instability, was the period in question caused by a temporarily upsetting condition such as a death, illness or marital breakup? If so, has the situation been resolved and is the applicant now emotionally stable?
- In the case of a criminal act, did someone pressure or coerce the applicant to commit the act? If so, is this person no longer present in the applicant's life? Can the applicant provide evidence that he or she did not commit the offense in question?
- In the case of improper handling of classified information, did the applicant respond favorably to counseling or remedial security training and does he or she now demonstrate

a positive attitude toward the discharge of security responsibilities? Was the violation a result of improper or inadequate training?

- In the case of an outside employment or activity, did the applicant terminate the employment or cease the activity upon learning that it was in conflict with his or her security responsibilities?
- In the case of information technology misconduct, was the misuse minor and done only in the interest of organizational efficiency and effectiveness, for example, another person using one's password or computer when no other timely alternative was readily available?

4. Why do I need an attorney?

If you are in the process of appealing an adverse security clearance decision, an attorney can assist you in framing your arguments consistent with the protocols listed above, in demonstrating that you have not violated the protocols, or in showing that the penalty is not consistent with your violation. You may also wish that an attorney represent you at your hearing and help you prepare for that hearing by gathering evidence and presenting it in a persuasive fashion. An attorney with experience examining and cross-examining witnesses can be invaluable during a hearing. An experienced attorney may also have handled security clearance cases with your particular agency, and will be able to frame your case consistent with your agency's expectations.

If you would like to discuss your issues regarding your security clearance, call *The Employment Law Group*® law firm at 888-603-0983 or contact us by email at inquiry@employmentlawgroup.com.