January 1988

Loss Or Denial of Security Clearance: An Employee's Rights

Katrina J. Church

Follow this and additional works at: http://digitalcommons.law.scu.edu/chtlj

Part of the Law Commons

Recommended Citation

This Article is brought to you for free and open access by the Journals at Santa Clara Law Digital Commons. It has been accepted for inclusion in Santa Clara High Technology Law Journal by an authorized administrator of Santa Clara Law Digital Commons. For more information, please contact sculawlibrarian@gmail.com.
ARTICLES

LOSS OR DENIAL OF SECURITY CLEARANCE: AN EMPLOYEE'S RIGHTS

Katrina J. Church*

TABLE OF CONTENTS

I. INTRODUCTION .................................. 198
II. STATUTORY LAW ............................... 200
   A. U.S. Constitution ............................ 200
   B. Executive Order 10865 ....................... 200
III. DEPARTMENT OF DEFENSE PROCEDURES ... 202
   A. Criteria for Granting Security Clearance
      Personnel Security Program .................. 202
   B. Review Process: Defense Industrial Personnel
      Security Clearance Review ................... 204
      1. Application ................................ 204
      2. Investigation .............................. 206
      3. Hearing: Post-Investigation ............... 207
      4. Written Findings; Determination .......... 209
   C. Administrative Loss of Clearance .......... 210
   D. Reinvestigation ............................ 211
   E. Administrative Review ...................... 212
      1. Appellate Process .......................... 212
      2. Reimbursement for Loss of Earnings .... 213
   F. Judicial Review ................................ 214
IV. DEPARTMENT OF ENERGY PROCEDURES ... 216
   A. Application .................................. 216
   B. Investigation ................................ 217
   C. Hearing: Post-Investigation ............... 217
   D. Written Findings; Determination .......... 219
   E. Reconsideration ............................ 221
V. CALIFORNIA WRONGFUL DISCHARGE
   LAWS ............................................. 222

* Associate, Hopkins & Carley, a law corporation, San Jose, California. J.D., New
I. INTRODUCTION

In September 1987, there were nearly 4,000,000 outstanding security clearances in the United States, granted by some 20 federal departments and agencies. The total value of defense contracts the previous year in Santa Clara County, California, alone was $4,155,996,000. Of the outstanding clearances, therefore, it stands to reason that a substantial number are held by employees of Silicon Valley companies, which act as contractors for the U.S. Department of Defense ("Defense Department" or "D.O.D.") and the U.S. Department of Energy ("D.O.E").

The nature of defense contracting is such that, without access to classified information, applicants at many levels cannot obtain work. Although having a security clearance does not guarantee access to classified information, access is granted only to persons with the appropriate clearance and whose official duties require such access. Security clearance is granted to employees of defense contractors because it has been determined that those positions require access to classified information. The corollary is that an employee whose security clearance is revoked and whose job entails access to classified information will be out of a job.

Under normal circumstances, a personnel security clearance remains valid until the individual has no further official relationship with the defense contractor or until "regular access to [that] level of classified information for which the individual holds a clearance is no longer necessary in the normal course of his or her duties." Several events can trigger a full reinvestigation, however, and peri-
One possible result is that the individual will not only be denied access to higher level classified information, but will lose any security clearance he then holds. The rationale behind this is not entirely clear, since the standards for Secret and Top Secret clearance are more stringent than the standards for Confidential clearance. Presumably, however, if access to classified information is not justified at the highest levels, it is not advisable at any level.

The case law in this area uniformly addresses the situation where some action on the part of the employee has — rightfully or wrongfully — resulted in the revocation or denial of that person's clearance for access to classified information. No cases have involved an act or omission on the employer's part which resulted in the revocation of an employee's security clearance. The practical effect of any revocation of clearance, however, is that finding another job with a defense contractor will be very difficult, and the employee will have to choose between working in another field within the industry, or working outside the industry. In Silicon Valley, that might not be a choice at all.

The Defense Department and the D.O.E. have somewhat different rules regarding the grant and review of security clearances. This article focuses on the Defense Department regulations, and then compares them with the D.O.E. procedures. The article's goal is to clarify for employees of defense contractors the remedies available to them upon revocation of their security clearance, and the criteria which the federal government agencies use to make such determinations. This article does not address the myriad of reasons for which an employee may lose his job or his remedies should removal be caused by any event other than loss of security clearance.

8. 32 C.F.R. § 155.3 See infra note 84 and accompanying text.
10. By contrast, Government employees in the "competitive service" are guaranteed that the fact that they are removed from employment on national security grounds will not preclude them from seeking or accepting employment in any other United States agency. 5 U.S.C.S. § 7312. "Competitive service" is defined as (1) all civil service positions in the executive branch except those positions (A) which are specifically exempted by some other statute, (B) which are confirmed by the Senate, or (C) with the Senior Executive Service; (2) all civil service positions not in the executive branch which are specifically included in the competitive service by statute; and (3) positions in the government of the District of Columbia which are specifically included by statute. Id. § 2102. "Competitive service" is the same as "classified [civil] service." Id. § 2102(c).
II. Statutory Law

A. U.S. Constitution

No person has a constitutional or statutory "right" to a security clearance. At the same time, the Fifth Amendment of the United States Constitution states that no person shall be deprived of life, liberty, or property without due process of law. This "due process clause" protects the "right to hold specific employment and to follow a chosen profession free from unreasonable governmental interference."

The national security reasons behind the grant or denial of security clearance were once believed to override the due process protection of the Constitution. Then in 1959, the U.S. Supreme Court was prevailed upon to decide the case of an aeronautical engineer whose industrial employment depended upon having access to classified information — and whose security clearance the Government attempted to revoke.

The action against the employee in Greene v. McElroy was based on certain confidential reports which were never made available to the employee, and the employee was given no opportunity to cross-examine adverse witnesses. The Supreme Court found that such proceedings were too far removed from traditional notions of due process to stand unless they were clearly authorized. The Court did not reach the constitutional issue, holding instead that there was no clear Congressional or Presidential authorization for the procedures, and that the attempted revocation of clearance failed on that basis.

B. Executive Order 10865

The following year, in the wake of the Greene decision, President Eisenhower issued Executive Order 10865, "Safeguarding Classified Information Within Industry" (the "Order"). The Order contains two basic premises. First, it sets the framework for the "Industrial Personnel Security Clearance Review Program," which

13. Id. The distinction between having a security clearance and being granted access to classified information is discussed infra text accompanying notes 86 & 87.
15. 360 U.S. at 479-480, 487, 79 S. Ct. at 1405, 1409.
16. Id. at 497, 79 S. Ct. at 1414.
17. Id. at 507-508, 79 S. Ct. at 1419.
is administered by the Department of Defense, and equivalent programs administered by other Government agencies. The Industrial Personnel Security Clearance Review Program is discussed below, at III(B). Second, the Order sets forth a minimum standard for the process due any employee whose security clearance may be denied or revoked. Employees of U.S. industries which contract with the Department of Defense are subject to the Order by virtue of the following language:19

[R]egulations prescribed by the Secretary of Defense under subsection (a) of this section may be extended to apply to protect releases (1) of classified information to or within United States industry that relate to bidding, or the negotiation, award, performance, or termination of contracts with [any] other department or agency [of the United States], and (2) other releases of classified information to or within industry, which such other department or agency has responsibility for safeguarding.

"Due process" under the Order consists of the following procedural safeguards:

1. a written statement of reasons why access to classified information may be denied or revoked ("Statement of Reasons");
2. an opportunity to reply in writing;
3. an opportunity for a hearing after filing a written reply to the Statement of Reasons;
4. reasonable time to prepare for the hearing;
5. the opportunity to be represented by counsel;
6. the opportunity to cross-examine persons on any matters (with a limitation on the disclosure of classified information) raised in the Statement of Reasons, other than the characterization of any organization or individual other than the applicant; and
7. written notice of the final decision concerning the allegations contained in the Statement of Reasons.20

The Order authorizes the Secretary of Defense to delegate to the Deputy or Assistant Secretary of Defense the responsibility for ensuring that access to classified information is available only if it is clearly consistent with the national interest.21 The Secretary of Defense is further authorized to "prescribe such specific requirements, restrictions, and other safeguards as [he] consider[s] necessary to protect (1) releases of classified information to or within United

20. Id. at § 3.
21. Id. at § 2.
III. DEPARTMENT OF DEFENSE PROCEDURES

A. Criteria for Granting Security Clearance: Personnel Security Program

The decision whether to grant personnel security clearance to employees of defense contractors has two stages. The second stage, relating to due process and the method of appeal, is the main focus of this Article. To understand that process, however it is necessary to understand the initial investigation and review process. This is so for two reasons: one, applications reach the appeal level only by virtue of a determination made at the investigation level, and two, much of the policy for the appeal process is established in the statute which governs initial investigation.

The employee of a defense contractor who requires security clearance to conduct his work must apply for that clearance through the Defense Industrial Personnel Security Clearance Review Program. Each applicant, defined as "a person in industry who requires a security clearance for access to classified information," is investigated in accordance with the standards of two Department publications: the Department of Defense Personnel Security Program and the Industrial Security Regulation.

The Personnel Security Program prescribes the Defense Department policy and procedures for granting access, as distinguished from reviewing the decision to grant access, to classified information and employment in sensitive positions by industry contractor personnel, and specifies the nature and extent of the investiga-

---

22. Id. at § 1(a).
23. "Defense Industrial Personnel Security Clearance Review Program," D.O.D. Directive 5220.6, 32 C.F.R. Part 155 (July 1, 1987 Ed.) (Part 155 was proposed to be amended on May 6, 1987, but the amendments still have not been adopted. Unless otherwise indicated, references are to the codification and not to the proposed rules.).
24. 32 C.F.R. § 155.3.
25. Id. § 155.6(a).
27. "Industrial Security Regulation," D.O.D. 5220.22-R. At the date of publication of this Article, the author has been unable to obtain a copy of D.O.D. 5220.22-R. Section 155.6 of D.O.D. Directive 5220.6 (7-86 Edition) instructed that copies could be obtained from the U.S. Naval Publications and Forms Center. That office informed the author that it did not have the document. As proposed to be amended on May 6, 1987, Section 155.6 instructs that requests for investigation under D.O.D. 5220.22-R should be submitted to the Office of the Under Secretary of Defense for Policy, Pentagon, Wash. D.C. 20301. 52 Fed. Reg. 18,865 (May 6, 1987).
The criteria applied in making the decision are reproduced at Appendix A to this Article.

Investigations under the Personnel Security Program are conducted by the Defense Investigative Service ("DIS") or the Defense Industrial Clearance Office ("DISCO"). DIS is a separate "law enforcement, personnel security investigative, and industrial security agency" of the Department of Defense under the direction, authority, and control of the Deputy Under Secretary of Defense for Policy. DIS administers the Defense Industrial Security Program ("Industrial Security Program"), and is responsible for security clearance investigations within the 50 States, the District of Columbia and the Commonwealth of Puerto Rico. The Director of DIS operates the Industrial Security Program as a separate element on behalf of all D.O.D. components. Within that structure, overall responsibility for policy and administration lies with the Deputy Under Secretary of Defense (Policy Review). DISCO is operated within DIS as a "consolidated central facility to process industrial security clearances."

As a rule, security clearance should be granted if, based on all available information, the applicant's loyalty, reliability, and trustworthiness are such that entrusting the person with classified information or assigning the person to sensitive duties is clearly

30. 32 C.F.R. § 361.3(a).
32. D.O.D. Directive 5105.42 supra note 29 assigns responsibility to DIS; 32 C.F.R. § 154.9(a) states the jurisdiction of the DIS.
33. D.O.D. Directive 5220.22(D)(3), supra note 31, at 1404. "D.O.D. Components" is defined generally as the Office of the Secretary of Defense; the Military Departments; Organization of the Joint Chiefs of Staff; and the Defense Agencies. 32 C.F.R. § 155.2(a); D.O.D. Directive 5220.22(B), supra note 31, at para. 700.10; 32 C.F.R. § 154.2(f) (the latter definition includes only the Directors, not other personnel, of Defense Agencies, and adds Directors of the Unified and Specified Commands).
36. Id. § 361.4(e).
consistent with the interests of national security.\textsuperscript{37}

Security clearance should be granted only to those persons who require access to classified information for "mission accomplishment," and only when such access is required in connection with official duties.\textsuperscript{38} The investigation is necessarily subjective, and the goal is simply to "judge whether the circumstances of a particular case, taking into consideration prior experience with similar cases, reasonably suggest a degree of probability of prejudicial behavior not consistent with the national security."\textsuperscript{39}

If clearance is granted, there is no further review. If clearance is denied (or revoked following a reinvestigation), the decision will be reviewed as set forth below.


1. Application

In 1966, the Department of Defense promulgated the D.O.D. Industrial Security Program, which implements Executive Order 10865, and established the Defense Industrial Personnel Security Clearance Review Program ("Clearance Review Program").\textsuperscript{40} By consent, the following agencies not otherwise associated with the Department of Defense participate in the Clearance Review Program:\textsuperscript{41}

- Department of Agriculture
- Department of Commerce
- Department of Interior
- Department of Justice
- Department of Labor
- Department of State
- Department of Transportation
- Department of Treasury
- Environmental Protection Agency
- Federal Emergency Management Agency
- Federal Reserve System
- General Accounting Office
- General Services Administration

\textsuperscript{37} \textit{Id.} §§ 154.6(b), 154.40(a).
\textsuperscript{38} \textit{Id.} § 154.16(1), (2).
\textsuperscript{39} \textit{Id.} § 154.40(b).
\textsuperscript{40} D.O.D. Directive 5220.22, \textit{supra} note 31; D.O.D. Directive 5220.6, \textit{supra} note 23.
\textsuperscript{41} 32 C.F.R. § 155.2(b).
National Aeronautics and Space Administration
National Science Foundation
Small Business Administration
United States Arms Control and Disarmament Agency
United States Information Agency

Notably absent is the Department of Energy, which is responsible for atomic weaponry, and which has promulgated independent regulations.\textsuperscript{42}

The Clearance Review Program covers requests for security clearance referred by the DIS or DISCO pursuant to the Personnel Security Program, and can be extended to other cases at the direction of the Deputy Under Secretary of Defense for Policy.\textsuperscript{43} If DIS or DISCO cannot affirmatively determine that it is “clearly consistent with the national interest to grant or continue a security clearance for access to classified information” by a person employed by U.S. industry,\textsuperscript{44} they refer the case to the Directorate for Industrial Security Clearance Review (“DISCR”) for action under the Clearance Review Program.\textsuperscript{45} The Clearance Review Program does not apply to an administrative revocation of security clearance, discussed below.\textsuperscript{46}

Any person in industry who requires a security clearance for access to classified information (defined as an “applicant” under the Clearance Review Program) is investigated in accordance with the standards set forth in the Personnel Security Program.\textsuperscript{47} The Personnel Security Program generally applies to investigations of contractor personnel and other personnel who are affiliated with the Department of Defense, but “unfavorable administrative action procedures” (adverse action taken as the result of security clearance determinations)\textsuperscript{48} are appealed in accordance with the procedures of the Clearance Review Program and the Industrial Security Regulation.\textsuperscript{49}

The Clearance Review Program contains a binding “adjudication policy” which controls any determination of eligibility for ac-

\textsuperscript{42} Greve, supra note 1, at 19A, col. 2. The regulations for the Department of Energy are found at 10 C.F.R. Parts 706, 710 and 725. The D.O.E. regulations are discussed infra text accompanying notes 141-184.
\textsuperscript{43} 32 C.F.R. § 155.2(e).
\textsuperscript{44} Id. § 155.2(e).
\textsuperscript{45} Id.; id. § 155.7(a).
\textsuperscript{46} Id. § 155.2(d). See infra text accompanying notes 86-96.
\textsuperscript{47} 32 C.F.R. §§ 155.6(a), 155.3.
\textsuperscript{48} Id. § 154.2(cc).
\textsuperscript{49} Id. § 154.2(b).
cess to classified information or assignment to sensitive duties. National security is paramount in any adjudication under the Clearance Review Program, and the standard for granting clearance is that to do so would be "clearly consistent with the interests of national security." The adjudication policy is keyed to the criteria for granting initial clearance.

2. Investigation

The Clearance Review Program essentially tracks the minimum due process standards set out in Executive Order 10865. DISCO reviews any person in U.S. industry who applies for security clearance. If DISCO determines that it is "clearly consistent with the national interest" for the person to have access to classified information, then there is no further review. If there is an adverse determination, the case is referred to DISCR for administrative review under the Clearance Review Program.

DISCR may investigate, direct written interrogatories, require psychiatric evaluation, conduct interviews with any individual whose security clearance is being considered, and finally, recommend suspension of security clearance. Pending completion of the investigation, the Deputy Under Secretary of Defense for Policy may suspend the applicant's security clearance with the concurrence of the Department of General Counsel ("D.O.D. Counsel"), if there is "sufficient information to provide a reasonable basis for concluding that an applicant's continued access to classified information could endanger the national interest."

During the course of investigation, written or oral statements adverse to the applicant may be received and considered without affording the applicant an opportunity to cross-examine if D.O.D. Counsel determines (a) that "the statement concerned appears to be reliable and material," (b) that failure to consider the statement "would be substantially harmful to the national security," and (c)

50. *Id.* § 155.6(f).
51. *Id.* § 155.8(a).
52. *Id.* The criteria for determining eligibility for clearance appear *id.* § 155.6(e), and are duplicated *id.* § 154.7. They are reprinted at Appendix A hereof.
53. *Id.* § 155.2(c). DISCO has investigative authority pursuant to 32 C.F.R. Part 361, and conducts its investigation in accordance with 32 C.F.R. Part 154.
54. 32 C.F.R. § 155.2(c).
55. *Id.* § 155.7(b).
56. *Id.* § 155.6(g). The roles of the Deputy Under Secretary of Defense for Policy and the D.O.D. General Counsel may be delegated to their "designees."
that the person who made the statement is unavailable to testify "due to some . . . cause determined by the Secretary of Defense, or when appropriate, by the agency head to be good and sufficient."57

If the head of the department supplying the statement certifies that disclosure of an informant's identity would be substantially harmful to the national interest, the D.O.D. Counsel is not required to make any determination as to admissibility of evidence supplied by the informant.58 Physical evidence other than classified investigative reports, which are unavailable for inspection by the applicant, may be received in evidence if D.O.D. Counsel determines that it appears to be material and that failure to receive and consider it would be "substantially harmful" to the national security.59 The Constitutional guarantee of due process is not triggered by this fact-finding investigation.60

3. Hearing: Post-Investigation

When the investigation is completed, DISCR must either (a) issue a written notice that it has determined that the applicant's access to classified information is "clearly consistent with the national interest" and rescind any suspension of the applicant's security clearance; or (b) serve the applicant with a Statement of Reasons which clearly outlines the further procedures available to the applicant, including the right to counsel.61 No security clearance may be revoked unless the applicant receives a written Statement of Reasons "as detailed and comprehensive as the national security permits."62

Upon receiving the Statement of Reasons, in order to be entitled to a hearing, the applicant must: (a) request a hearing, and (b) reply in writing to the Statement of Reasons.63 The reply must admit or deny each listed allegation (a general denial is not sufficient), must be specific, and must be submitted to DISCR within 20 days of receipt of the Statement of Reasons.64 If the applicant fails to answer the Statement of Reasons in a responsive manner, the Director of DISCR will deny the requested clearance and any clearance

57. 32 C.F.R. § 155.6(i).
58. Id.
59. Id. § 155.6(h).
61. Id. 32 C.F.R. § 155.7(c).
62. Id.
63. Id. § 155.7(d).
64. Id. The applicant may petition the Director of DISCR for a "reasonable extension."
then held by the applicant will be administratively suspended.\textsuperscript{65}

If the applicant answers the Statement of Reasons but does not request a hearing — and if counsel to DISCR does not request a hearing — the Examiner (an attorney assigned to DISCR to conduct hearings and reach clearance determinations)\textsuperscript{66} will make a determination regarding the applicant's security clearance based upon a review of the file of "all relevant material."\textsuperscript{67} A copy of that file is provided to the applicant, who then has twenty days to submit a rebuttal in the form of documentary information, or to explain any adverse information in the file. After receiving the file, the applicant may not change his mind and elect to have a hearing.\textsuperscript{68}

If a review of the applicant's reply to the Statement of Reasons indicates that all the allegations are unfounded, or if there is insufficient evidence to proceed in accordance with the adjudication policy, the Director of DISCR will take action "as appropriate under the circumstances."\textsuperscript{69} The applicant must be notified in writing of either of these actions taken without a hearing.\textsuperscript{70}

If the applicant answers the Statement of Reasons responsive, and if the applicant or counsel to DISCR requests a hearing, the hearing takes place before Examiners, who are designated by D.O.D. Counsel.\textsuperscript{71} This hearing meets all the procedural safeguards required by Executive Order 10865.\textsuperscript{72} The applicant has the right to counsel, to present evidence, and generally to cross-examine adverse witnesses.\textsuperscript{73} All parties to the hearing are served with a copy of any pleading or communication at the time it is submitted to the Examiner.\textsuperscript{74} The applicant's failure to appear or proceed "in a timely and orderly fashion," or failure or refusal to answer or authorize others to answer relevant material questions will result in dismissal of the case, denial of any pending request for clearance, and suspension of any security clearance then held by the applicant.\textsuperscript{75}

D.O.D. Counsel is responsible for producing the witnesses and information upon which DISCR has relied to establish controverted

\begin{footnotes}
\footnotetext{65. Id. § 155.7(f).}{\footnotemark[65]}
\footnotetext{66. Id. § 155.5(b)(4).}{\footnotemark[66]}
\footnotetext{67. Id. § 155.7(e).}{\footnotemark[67]}
\footnotetext{68. Id.}{\footnotemark[68]}
\footnotetext{69. Id. § 155.7(f).}{\footnotemark[69]}
\footnotetext{70. Id.}{\footnotemark[70]}
\footnotetext{71. Id. § 155.5(b).}{\footnotemark[71]}
\footnotetext{72. See generally id. § 155.7; Greene v. McElroy, 360 U.S. at 474.}{\footnotemark[72]}
\footnotetext{73. 32 C.F.R. § 155.7(g).}{\footnotemark[73]}
\footnotetext{74. Id. § 155.7(i).}{\footnotemark[74]}
\footnotetext{75. Id. § 155.7(j).}{\footnotemark[75]}
\end{footnotes}
facts alleged in the Statement of Reasons. As dictated by the evidence presented, the Statement of Reasons may be amended at the hearing to make it conform to the information or evidence presented, and the applicant may have additional time to answer the amendments and to present evidence.

The Federal Rules of Evidence are used in these hearings only as a guide, so that a full record may be developed without technical omissions. Thus, any relevant and material oral, documentary, or other evidence may be received. Information furnished by an investigative agency pursuant to its responsibilities in assisting to safeguard classified information with the industry may also be received in evidence, provided that such information consists of records compiled in the regular course of business or other physical evidence other than investigative reports.

4. Written Findings: Determination

After the hearing, the applicant and D.O.D. Counsel receive a transcript. The Examiner must make written findings with respect to each allegation in the Statement of Reasons, together with reasons supporting those findings, within thirty days following the close of the hearing record. The Examiner’s determination is based on the standard of whether it is clearly consistent with the national interest to grant or continue the applicant’s eligibility for access to classified information. The Examiner’s determination may be appealed. Every determination, favorable or otherwise, is entered into an automated subsystem of the Defense Central Index of Investigations, and that record will be consulted the next time the applicant requests renewed or higher clearance.

76. Id. § 155.7(k).
77. Id.
78. Id. § 155.7(n); but see Gayer v. Schlesinger, 490 F.2d 740, 747, at n.13 (D.C. Cir. 1973), citing Camero v. United States, 375 F.2d 777 (Ct. Cl. 1967) (“In providing for an adversary agency hearing traditional requirements assuring a fair and impartial adjudication are to be complied with, notwithstanding [former] 32 C.F.R. § 155.7(c)(1) which states with respect to such hearings, the rules, including the rules of evidence, are not applicable to hearings under this part.”).
79. 32 C.F.R. § 155.7(c).
80. Id. § 155.7(o).
81. Id. § 155.7(q).
82. See infra text accompanying notes 106-119.
83. Id. § 154.43(a), § 154.2(e).
C. Administrative Loss of Clearance

A basic premise of both the Personnel Security Program and the Clearance Review Program is that security clearance will be revoked or downgraded administratively when the government contractor no longer does work which requires that its employees have access to classified information, or when the employee is transferred to another location or job which does not require such access, or which requires only lower-level access. Access to confidential information by industrial and commercial entities is permitted only to personnel who have the requisite security clearance, and then only if access is “essential to a function that is necessary in the interest of the national security.” The applicant must be cleared in accordance with the Industrial Security Regulations. Employees whose duties no longer require access to classified information are not eligible for security clearance.

The Personnel Security Program dictates that the number of people with security clearances should be kept to a minimum, as required by the specific job. “Special attention” is to be given to “eliminating unnecessary clearances.” Among those who are not eligible for clearance are persons whose regular duties do not require authorized access to classified information, even for their ease of movement within restricted, controlled, or industrial areas, and persons who can be prevented from accessing classified information by being escorted by cleared personnel. In 1985, then-Defense Secretary Caspar Weinberger announced his decision to eliminate ten percent of the security clearances at defense firms. Many companies were able to meet the quota simply by culling those clearances held by employees who no longer worked on classified programs and no longer required clearances. Those employees

84. Id. § 154.50. See also Maggrett, “More Than 5,500 People Have Unwarranted Access to D.O.E.,” 27 Nucleonics Week, July 17, 1987, No. 29, at 5, reprinted from NEXIS (information from D.O.E. Inspector General’s report indicates that “D.O.E. policy requires that clearances be withdrawn on employee termination or transfer to areas where clearance is unnecessary.”). The Department of Energy is responsible, among other duties, for making the Pentagon’s nuclear weapons. Greve, supra note 1, at 19A, col. 2.
85. 32 C.F.R. § 159.70(f)(4).
86. Id; see also 32 C.F.R. § 154.13(d) (“If an individual departs from a Top Secret billet to a billet/position involving a lower level clearance, the Top Secret Clearance will be administratively rescinded.”).
87. 32 C.F.R. § 154.10(b).
88. 32 C.F.R. § 154.16(f). See, e.g., Johnson, Silicon Valley Firms With Defense Contracts Given Fewer Clearances,” S.J. Mercury News, Sept. 6, 1987, at A19, col. 1 (defense consultant whose clearance was revoked had to be escorted to the bathroom).
89. Johnson, supra note 90, at A18, col. 1.
90. Johnson, at A18, col. 2.
have not been deprived of the right to hold specific employment free from unreasonable governmental interference, since they continue to be employed at their old jobs.

An employee has no statutory remedy if security clearance is revoked on the grounds that access to classified information is no longer warranted or necessary. The Clearance Review Program does not apply to administrative withdrawal of a security clearance without prejudice (i.e., where no finding is made which might influence a later determination as to whether the applicant's access to classified information would be clearly consistent with the national interest).\textsuperscript{91}

A clearance which has been administratively suspended can be reinstated only upon a request submitted by the applicant to the Director of DISCR, and upon a showing of good cause. Only D.O.D. Counsel or his designee can approve such a request.\textsuperscript{92}

Employees of civilian defense contractors whose loss of security clearance also results in the loss of a job are eligible for unemployment compensation benefits.\textsuperscript{93}

\section*{D. Reinvestigation}

An employee can move to other companies in the defense contractor industry without having to reapply for a new security clearance if he finds employment within 12 months.\textsuperscript{94} All D.O.D. offices will reciprocally accept without additional investigation a determination permitting access to classified information made by authorized Defense Department authorities,\textsuperscript{95} a fact which enables employees to move to jobs with different contractors. Reciprocity with the Nuclear Regulatory Commission and the Department of Energy is governed by a separate document, D.O.D. Directive 5210.2.\textsuperscript{96}

The following events, however, can trigger a full reinvestigation of an individual's right to access to classified information:\textsuperscript{97}

\begin{itemize}
  \item \textsuperscript{91} 32 C.F.R. § 155.2(d).
  \item \textsuperscript{92} Id. § 155.7(c).
  \item \textsuperscript{94} 32 C.F.R. § 154.14(a), § 154.24.
  \item \textsuperscript{95} Id. § 154.25(a).
  \item \textsuperscript{96} Id. § 154.26(c).
  \item \textsuperscript{97} Id. § 154.19. There are additional categories which apply only to specified D.O.D. or NATO personnel.
\end{itemize}
1. any allegation related to the disqualification criteria outlined in the statute, with respect to an individual holding a security clearance;
2. periodic (five-year) reinvestigation of employees of contractors whose duties include any of the following:
   a. access to sensitive compartmented information;
   b. extraordinary sensitive duties;
   c. access to very sensitive information classified Secret;
   d. access to Top Secret information; and
   e. personnel occupying computer positions designated ADP-1;
3. to assess the current eligibility of individuals who were denied clearance after an initial investigation if a potential need for clearance exists;
4. break in employment of greater than twelve months;\(^98\)
5. consideration for a higher level clearance or special access authorization.\(^99\)

Furthermore, if any check of the Defense Central Index of Investigations (a system which contains, among other information, a record of every issuance, denial or revocation of security clearance and access to classified information\(^100\)) reveals any “derogatory information” accumulated against a person since his last security determination, the person will be reinvestigated.\(^101\) “Derogatory information” is not defined in the statute, but “significant derogatory information” is any information that “could, in itself, justify an unfavorable administrative action, or prompt an adjudicator to seek additional investigation or clarification.” “Unfavorable administrative action” is adverse action taken as the result of personnel security determinations under the statute.\(^102\)

E. Administrative Review

Administrative review of the denial or revocation of a security clearance is dictated by the provisions of the Clearance Review Program and Executive Order 10685.

1. Appellate Process

Within twenty days after the Hearing Examiner makes a determination, which must be in writing and copies of which must be

---

\(^{98}\) Id. § 154.25(a).

\(^{99}\) Id. § 154.25(b)(2).

\(^{100}\) Id. § 154.2(c); see supra text accompanying note 84.

\(^{101}\) Id. § 154.25(a).

\(^{102}\) Id. § 154.3(x), (cc).
provided to the applicant and D.O.D. Counsel, either party may file a written Notice of Appeal with the Director of DISCR, signifying their intention to appeal the determination.\textsuperscript{103} The appeal must also be written, and must be filed with DISCR within sixty days after the date of the determination.\textsuperscript{104} The appeal must state the specific issues raised, must cite those portions of the case record which support the issues, and must state reasons why the determination should be reversed.\textsuperscript{105} Appeal is limited to whether\textsuperscript{106} the Examiner's rulings were arbitrary or capricious. The appeal will be heard with respect to the case record and issues raised on appeal, without reference to new testimony or evidence.\textsuperscript{107}

The appeal is submitted to the Appeal Board for consideration.\textsuperscript{108} The Appeal Board, which is a panel of attorneys designated by the General Counsel to make final determination,\textsuperscript{109} decides only matters of law, and will not review the record \textit{de novo} or substitute its judgment for that of the Examiner.\textsuperscript{110}

The Appeal Board issues a final determination in writing which either affirms the Examiner's determination or returns the case to the Examiner with instructions for further action.\textsuperscript{111} The Appeal Board's written determination is provided to both parties.\textsuperscript{112} If the case was decided on information to which the applicant was denied access, only the Secretary of Defense or the agency head may make a final determination based upon a personal review of the case.\textsuperscript{113}

2. Reimbursement for Loss of Earnings

An applicant to whom DISCR later grants security clearance after clearance has once been suspended, denied or revoked, may petition the D.O.D. Counsel for reimbursement of loss of earnings resulting directly from the suspension, revocation, or denial of clearance.\textsuperscript{114}

Claims for reimbursement must be filed "within one year after

\begin{footnotesize}
\begin{enumerate}
  \item Id. § 155.7(r).
  \item Id.
  \item Id. § 155.7(s).
  \item Id.
  \item Id. § 155.7(t).
  \item Id. § 155.7(u).
  \item Id. § 155.5(b).
  \item Id. § 155.7(s).
  \item Id. § 155.7(u).
  \item Id.
  \item Id.
  \item 32 C.F.R. § 155.7(u).
  \item Id. § 155.7(w).
\end{enumerate}
\end{footnotesize}
the date the claim arises,” which is the date on which DISCR ultimately grants security clearance.115

The petitioner will not be reimbursed if, in the D.O.D. Counsel view, the Department of Defense was justified in taking the initial action to suspend, deny, or revoke clearance.116 Claims for reimbursement from agencies other than the Defense Department are forwarded to that agency.117

The amount of reimbursement for lost earnings is reduced by the amount the petitioner was able to earn in the interim period, subject to “reasonable efforts” on the applicant’s part to mitigate any loss of earnings.118 Interim earnings include any unemploy-

ment compensation payments the petitioner received, and the peti-
tioner will not be reimbursed for any period during which loss of earnings was caused by undue delay resulting from the petitioner’s acts or failure to act.119

F. Judicial Review

An employee who has exhausted his administrative remedies still has recourse in the courts. Generally, “judicial review of factual determinations by agencies is limited to whether, considering the record as a whole, there is substantial evidence supporting the findings.”120 The court will not make a new factual determination based on its interpretation of the evidence, and will only determine whether the administrative action was justified.

In February 1988, the U.S. Supreme Court redefined the role of the courts in reviewing the revocation of security clearance. Specifically, in Department of the Navy v. Egan,121 the Court held that the Merit Systems Protection Board does not have authority to rule on the substance of an underlying security-clearance determination in the course of reviewing an “adverse action.”

The case began when Thomas Egan was removed from his job at the Trident Naval Refit Facility following denial of security

115. Id. § 155.7(w).
116. Id. § 155.7(w).
117. Id. § 155.7(y).
118. Id § 155.7(x).
119. Id.; Kanarek v. United States, 394 F.2d 525, 527 (Ct. Cl. 1968).
121. — U.S. —, 108 S. Ct. 818 (1988). The case concerns a different area of the United States Code, specifically Title 5, sections 7513 and 7532. That statute governs government employees in the competitive service, see supra text accompanying note 10. Basic analogies can be drawn to statutes governing defense industrial contractor personnel, however.
clearance. It had been made clear to him that his job was contingent on obtaining such clearance. Egan appealed to the Personnel Security Appeals Board, which affirmed denial of his security clearance.

He sought review of his removal (not the denial of his clearance) by the Merit Systems Protection Board ("Merit Board"), which affirmed the action. The Court of Appeals reversed, saying that the Merit Board could review the merits of the underlying determination. The Supreme Court reinstated the Merit Board decision. The court found that the Merit Board was authorized only to review an "adverse action," defined in the statute to include removal, suspension for more than fourteen days, reduction in grade or pay, and furlough of thirty days or less. The Merit Board may only determine whether the adverse action was taken for cause. In this instance, the "cause" for Egan's removal was denial of security clearance. The Court held that the Merit Board was not authorized to take the additional step of determining whether the denial was itself justified.

This ruling arguably begs the question: how does the Merit Board prevent arbitrary removal if it may not determine whether the "cause" for removal is real or capricious. As noted elsewhere in this Article, the decision to grant or deny a security clearance is necessarily subjective. On those grounds, the Court declined to second-guess the agency normally entrusted with that decision. "Certainly," wrote Justice Blackmun for the majority,

it is not reasonably possible for an outside nonexpert body to review the substance of such a judgment and to decide whether the agency should have been able to make the necessary affirmative prediction [of possible future behavior] with confidence. Nor can such a body determine what constitutes an acceptable margin of error in assessing the potential risk.

The Egan case does not precisely define the level of judicial review for decisions of the Personnel Security Appeals Board. Nevertheless, the Court has emphasized the doctrine of separation of powers, finding that "the grant of security clearance to a particular employee, a sensitive and inherently discretionary judgment call, is committed by law to the appropriate agency of the Executive

122. Id. at 820.
123. Id. at 825.
125. Id. at 825.
126. Id.
Branch." 127 Such language makes it unlikely that an employee can get judicial review on the merits of a denial or revocation of security clearance.

Although the court's role is one of judicial restraint, however, it will not hesitate to intervene to prevent "arbitrary and unreasonable governmental action." A court will look for a "rational relationship" between the applicant's conduct and the actions taken by the administrative body. 128 If the applicant has cooperated fully, the burden will be on the government to prove that rational nexus. 129

IV. DEPARTMENT OF ENERGY PROCEDURES

A. Application

The statute which implements Executive Order 10865 for the Department of Energy is entitled "Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Significant Quantities of Special Nuclear Material". 130 It applies to questions of eligibility for access to "Restricted Data or significant quantities of special nuclear material" involving employees of and applicants for employment with contractors and agents of the D.O.E. 131

The D.O.E. statute is not much different from the Defense Department statute in substance, although it is clearer and easier to follow. The D.O.E. standard for granting clearance (called "access authorization") is a "comprehensive, commonsense judgment" as to whether granting access "would endanger the common defense and security and would be clearly consistent with the national interest." 132 The criteria which the D.O.E. generally applies (i.e., the "principal types of derogatory information" which pose a question regarding eligibility for access) are reprinted at Appendix B to this

127. Id. at 824.
129. 384 F. Supp. at 1379.
131. 10 C.F.R. § 710.1(a), § 710.2(a). "Restricted Data" is defined at 10 C.F.R. § 725.3(h) as "all data concerning (1) design, manufacture or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to section 142 of the [Atomic Energy Act of 1954]." Part 725 governs permits for access to Restricted Data. "Significant quantities of special nuclear material" is defined at 10 C.F.R. § 710.5(b), and includes a variety of radioactive and other chemical elements.
132. 10 C.F.R. § 710.10(a).
Article. The D.O.E. warns that these criteria are not exhaustive, nor is the D.O.E. precluded from deciding that information or facts are derogatory "although at variance with, or outside the scope of, the stated categories."133

B. Investigation

If information furnished to the D.O.E. creates a question as to an individual's eligibility for access authorization, the matter is turned over to the Manager of Operations at the D.O.E. Operations Office. The Manager of Operations may conduct interview or further investigation as he deems appropriate, and may authorize the access authorization. If the question of eligibility cannot be resolved through further investigation and psychiatric evaluation, the Manager of Operations must forward the case to the Director of the Office of Safeguards and Security of the D.O.E. 134 That office then has thirty days to grant access authorization, direct further investigation, or authorize hearing procedures in accordance with the statute. 135

C. Hearing: Post-Investigation

If interviews and other investigation cannot resolve a question as to eligibility for access authorization, the statute dictates procedures to be followed in the conduct of hearings.136 Pending a final determination, the Manager of Operations may suspend any current access authorization of the individual. In reaching this decision, he/she should consider such factors as the seriousness of the derogatory information developed, the individual's possible access to classified information or significant quantities of special nuclear material, and the individual's opportunity to commit acts adversely affecting the national security.137 The Manager of Operations must immediately notify the Assistant for Defense Programs of any suspension of access authorization, and within ten days must submit a request for authority to conduct a hearing to the Director, Office of Safeguards and Security. The request must contain an explanation of the basis for the suspension.138

Within thirty days after the Director authorizes review proce-

133. Id. § 710.10(b).
134. Id. § 710.10(c).
135. Id.
136. Id. § 710.20 et seq.
137. Id. § 710.21.
138. Id.
dures, the Manager of Operations must notify the individual in writing that "reliable information in [his] possession . . . has created a substantial doubt concerning the individual's eligibility to access authorization" and outlining procedures for the person to follow if he wishes to request a hearing. 139 The person must be given additional information and a copy of the statute. 140

If the individual does not request a hearing within twenty days after receiving the notification letter, the Manager of Operations will recommend to the Assistant Secretary for Defense Programs the final action to be taken on the basis of the information in the case. 141

If the individual timely requests a hearing, the Manager of Operations will assign a D.O.E. attorney to act as Hearing Counsel, to prepare and conduct hearings as provided in the statute. 142 Once arrangements have been made with the individual (or counsel for the individual) for an "expeditious hearing," the Hearing Officer will consider the evidence, make specific findings as to the truth of the derogatory information, and determine whether to recommend the grant, denial, or revocation of access authorization. 143

The individual may challenge the Hearing Officer for cause within seventy-two hours after being notified of the Hearing Officer's identity. The Manager of Operations will rule on the challenge and, if need be, appoint a new Hearing Officer who may also be challenged. 144

The individual will receive at least one week's notice of the hearing. If he/she fails to appear, the Manager of Operations will recommend final action based on the record to date. The hearing can be rescheduled upon a showing of good cause. 145

The Hearing Officer proceedings must commence a hearing within ninety days from the date the request for a hearing is received. 146 Throughout, the statute emphasizes that the proceeding is an administrative hearing and not a trial. As with the D.O.D. procedures, the Federal Rules of Evidence serve only as a guide. 147

Hearings are open only to duly authorized staff of the D.O.E., the

139. Id. § 710.22.
140. Id. § 710.23.
141. Id. § 710.24(a).
142. Id. § 710.25(a), § 710.5(e).
143. Id. § 710.26(a), § 710.5(g).
144. Id. § 710.26(c), § 710.26(d).
145. Id. § 710.26(e).
146. Id. § 710.27(a).
147. Id. § 710.27(g); see supra text accompanying note 79.
individual, counsel, and such other people as the Hearing Officer may authorize.  

During the course of the proceedings, the notification letter may be amended to correspond to the evidence received. Generically, the record may not contain any information adverse to the individual unless that information has been made available to the individual and he either has no objection to presentation of the information or he is afforded the opportunity to cross-examine the person providing the information. The exceptions to this right of cross-examination are the same as those under D.O.D. procedures discussed above. Unlike the D.O.D. procedures, however, the D.O.E. specifies that when the individual is denied access to information or adverse witnesses, he must be provided with a summary of the information “as comprehensive and detailed as the national security permits,” and appropriate weight is to be given to the fact that the individual was denied the right to confront the witnesses. Records and other physical evidence may be received on terms substantially similar to the D.O.D. procedures. Again, the individual is to be provided with a summary or description of any evidence which he is prohibited to inspect, to the extent that national security permits.

A transcript of the hearings is prepared and, except for portions containing Restricted Data or national security information, a copy furnished to the individual.

D. Written Findings: Determination

The Hearing Officer makes specific findings as to each allegation contained in the notification letter, and must support each finding with a statement of his reasons for such findings. The Hearing Officer bases his recommendation on whether he is of the opinion that granting access authorization “will not endanger the common defense and security and will be clearly consistent with the

148. Id. § 710.27(b); cf. 32 C.F.R. § 155.7(b) (“Hearings will be closed to spectators except upon mutual agreement of applicant and D.O.D. Counsel based on the necessity to protect classification information or other good cause”).
149. 10 C.F.R. § 710.27(f).
150. Id. § 710.27(k).
151. Id. § 710.27(m); see supra text accompanying notes 58 & 59.
152. 10 C.F.R. § 710.27(n).
153. Id. § 710.27(o), § 710.27(p); see supra text accompanying note 60.
154. 10 C.F.R. § 710.27(p)(3).
155. Id. § 710.27(r).
156. Id. § 710.28(b).
national interest." The Hearing Officer must submit his recommendation to the Manager of Operations within thirty days of the later of (a) receipt of the transcript, or (b) the closing of the record. New evidence can be heard if it is discovered prior to final determination of eligibility for access authorization.

The Manager of Operations transmits the Hearing Officer's findings and recommendation to the Assistant Secretary for Defense Programs through the Director of the Division of Safeguards and Security. If the Hearing Officer has recommended that access authorization be denied, the Manager of Operations must also submit a statement of the effect of such denial on the energy research and development program.

If the Hearing Officer recommends that access authorization be denied, the individual will immediately be notified of that fact and may request that his case be reviewed by the D.O.E. Personnel Security Review Examiner. The request for review must be submitted within five days to the Assistant Secretary for Defense Programs, and a brief supporting the individual's position should be submitted to the Assistant Secretary within ten days, via the Director of the Division of Safeguards and Security. If the individual does not request review within the prescribed period of time, the final determination will be made on the basis of the records and all findings and recommendations.

The Assistant Secretary of Defense Programs designates three D.O.E. Personnel Security Review Examiners to review the record of the case. The Examiners conduct their reviews independently of one another, and prepare individual reports of findings and recommendations for the Assistant Secretary. Each finding and recommendation must be fully supported by stated reasons for those conclusions, and Examiners generally submit reports within forty-five days after they are assigned the case.

Based on the record and all recommendations, the Assistant Secretary for Defense Program makes a final determination as to whether access authorization should be granted or denied. If the

157. Id. § 710.28(c).
158. Id. § 710.28(d).
159. See id. § 710.29.
160. Id. § 710.30(b).
161. Id.
162. Id. § 710.30(d)(1).
163. Id. § 710.30(d)(3).
164. Id. § 710.31(a), § 710.31(d).
165. Id. § 710.31(d).
decision is to deny access authorization, the Assistant Secretary will so notify the individual through the Manager of Operations and include his findings with respect to each allegation contained in the notification letter.\footnote{166}

If the individual has been denied the opportunity to confront and cross-examine witnesses who have furnished information adverse to him, and if the Assistant Secretary for Defense Programs reaches an adverse recommendation, the Secretary (head of the D.O.E.) will personally review the record and make a final determination.\footnote{167} A decision to revoke or deny access authorization will be forwarded to the individual on the same terms as above.\footnote{168}

E. \textit{Reconsideration}

1. When Access Authorization Granted

If the Assistant Secretary for Defense Programs or the Secretary has made a determination granting access authorization, eligibility will only be reconsidered if there is new "substantially derogatory information" or a "significant increase in the scope or sensitivity of the Restricted Data or national security information to which the individual has or will have access."\footnote{169} If the Manager of Operations granted access authorization without recourse to the hearing procedures, the determination can also be reconsidered with the specific prior approval of the Director of the Division [sic] of Safeguards and Security of the D.O.E.\footnote{170}

2. When Access Authorization Denied or Revoked

A determination denying access authorization will be reconsidered under the following circumstances:\footnote{171}

(a) the individual has received a bona fide offer of employment requiring access to Restricted Data, national security information, or significant quantities of special nuclear material; and

(b) there is either

(f) material and relevant new evidence which the individual and his representatives are not at fault in failing to present earlier, or

\footnotesize{\begin{itemize}
  \item[166.] \textit{Id.} § 710.32(a), § 710.32(c).
  \item[167.] \textit{Id.} § 710.33(a).
  \item[168.] \textit{Id.} § 710.33(b); see \textit{supra} text accompanying note 177.
  \item[169.] \textit{Id.} § 710.34(a).
  \item[170.] \textit{Id.} § 710.34(c).
  \item[171.] \textit{Id.} § 710.34(b).
\end{itemize}}
(ii) convincing evidence of the individual's reformation or rehabilitation.

Requests for reconsideration should be submitted in writing to the Assistant Secretary for Defense Programs through the Manager of Operations with jurisdiction over the position for which access authorization is required. The request must be accompanied by an affidavit setting forth in detail the new evidence of reformation or rehabilitation.172

The process for judicial review is the same as for any other administrative action.173 No provision is made for reimbursement of lost earnings.

V. CALIFORNIA WRONGFUL DISCHARGE LAWS

In California, an employment with no specific term may be terminated at the will of either party, upon notice to the other party.174 Absent agreement to the contrary, an employer may terminate an at will employment having no specified term, with or without cause.175 The terms of the individual contract may vary these rules, and the employer is bound to follow its own internal regulations.176 A contract for a specified term of employment may also be terminated upon notice of the occurrence of a specified condition to the employment.177 It could be argued however that recission of an employee's security clearance through no fault of the employee's but due to some act of the employer constitutes constructive discharge.178

The employee's remedy for a perceived wrongful discharge is an action in tort for wrongful discharge, or a combined action in tort and contract for the employer's breach of the implied covenant

172. Id.
173. See supra text accompanying notes 131-140.
175. Id. 29 Cal. Jur. 3d, Employer and Employee § 62 and cases cited therein.
178. See, e.g., Billetter v. Posell, 94 Cal. App. 2d 858, 211 P.2d 621 (1949) (notification that employee's wages and position have been reduced below what contract calls for is constructive discharge); Gregg v. McDonald, 73 Cal. App. 748, 239 P. 373 (1925) (discharge from the position one is employed to fill is a discharge from employment); 63 ALR 3d 539, "Reduction in rank or authority or change in duties as breach of employment contract."
of good faith and fair dealing. Before turning to the courts with any action, the employee must first exhaust all administrative remedies.

VI. CONCLUSION

The decision to grant security clearance and access to classified information to an individual reflects "an attempt to predict [the individual's] possible future behavior and to assess whether, under compulsion of circumstances or for other reasons, he might compromise sensitive information." Such a prediction cannot be made with any degree of certainty. For this reason, and because of the doctrine of separation of powers, the courts are content to allow the executive branch broad discretion in determining who may have access to classified information.

Due to the imprecise nature of the decision, an elaborate procedural mechanism has been devised in an attempt to make the process reasonably objective. Thus, in the Defense Department, the Personnel Security Program sets standards for granting clearance, and the Clearance Review Program establishes a review process for any adverse determination. The Department of Energy has an equivalent system.

Reasonable people may differ on the criteria to which the standard of "clearly consistent with the interests of the national security" is applied. For instance, in light of the 1987 incident in which U.S. Marine guards were seduced by Soviet women while KGB agents gained access to the U.S. Embassy in Moscow, the military's insistence that homosexuality predisposes one to vulnerability to coercion or blackmail seems outdated. Nevertheless, the courts will not substitute their own criteria for that developed by the agencies responsible for classified information.

An employee of an industrial defense contractor whose clearance is either denied or revoked has the same remedies whether the cause was an act or omission of the employee, or an act or omission

181. Egan, at 824.
182. Id. at 825.
of the employer. But if the employer has denied or revoked clearance without cause, i.e., if the employee still requires access to classified information in order to perform his job, and none of the criteria for determining eligibility for clearance apply to him, then the employee has a very good chance of succeeding on the merits in an appeal. The employer will be required to present evidence supporting his decision, and clearance will be granted or reinstated if the allegations are unfounded. Although the statutes and the courts allow broad discretion, they do not permit an employer to make arbitrary and capricious decisions. And, if the employer’s allegations are found to cast some doubt over whether the employee’s access to classified information is clearly consistent with the interests of national security, the employee still has recourse in the laws of wrongful discharge. In either case, the employee is assured due process under the law.
The criteria for determining eligibility for clearance under the standard [of clearly consistent with the national interest] shall include, but not be limited to the following:

1. Commission of any act of sabotage, espionage, treason, terrorism, anarchy, sedition, or attempts thereof or preparation thereof, or conspiring with or aiding or abetting another to commit or attempt to commit any such act.

2. Establishing or continuing a sympathetic association with a saboteur, spy, traitor, seditionist, anarchist, terrorist, revolutionist, or with an espionage or other secret agent or similar representative of a foreign nation whose interests may be inimical to the interest of the United States, or with any person who advocates the use of force or violence to overthrow the Government of the United States or to alter the form of the Government of the United States by unconstitutional means.

3. Advocacy or use of force or violence to overthrow the Government of the United States or to alter the form of government of the United States by unconstitutional means.

4. Knowing membership with the specific intent of furthering the aims of or adherence to and active participation in any foreign or domestic organization, association, movement, group or combination of persons (hereafter referred to as organizations) which unlawfully advocates or practices the commission of acts of force or violence to prevent others from exercising their rights under the Constitution or laws of the United States or of any State or which seeks to overthrow the Government of the United States or any State or subdivision thereof by unlawful means.

5. Unauthorized disclosure to any person of classified information, or of other information, disclosure of which is prohibited by Statute, Executive Order, or Regulation.

6. Performing or attempting to perform one's duties, acceptance and active maintenance of dual citizenship, or other acts conducted in a manner which serve [sic] or could be expected to serve the interests of another government in preference to the interests of the United States.

7. Disregard of public law, Statutes, Executive Orders or Regulations, including violation of security regulations or practices.
(8) Criminal or dishonest conduct.

(9) Acts of omission or commission that indicate poor judgment, unreliability or untrustworthiness.

(10) Any behavior or illness, including any mental condition, which, in the opinion of competent medical authority, may cause a defect in judgment or reliability with due regard to the transient or continuing effect of the illness and the medical findings in such case.

(11) Vulnerability to coercion, influence, or pressure that may cause conduct contrary to the national interest. This may be the presence of immediate family members or other persons to whom the applicant is bonded by affection or obligation in a nation (or areas under its domination) whose interests may be inimical to those of the United States, or any other circumstances that could cause the applicant to be vulnerable.

(12) Excessive indebtedness, recurring financial difficulties, or unexplained affluence.

(13) Habitual or episodic use of intoxicants to excess.

(14) Illegal or improper use, possession, transfer, sale or addiction to any controlled or psychoactive substance, narcotic, cannabis or other dangerous drug.

(15) Any knowing and willful falsification, cover-up, concealment, misrepresentation, or omission of a material fact from any written or oral statement, document, form or other representation or device used by the Department of Defense or any other Federal agency.

(16) Failing or refusing to answer or to authorize others to answer questions or provide information required by a Congressional committee, court of agency in the course of an official inquiry whenever such answers or information concern relevant and material matters pertinent to an evaluation of the individual's trustworthiness, reliability, and judgment.

(17) Acts of sexual misconduct or perversion indicative of moral turpitude, poor judgment, or lack of regard for the laws of society.
Appendix B
Eligibility Criteria for Clearance

Department of Energy

The principal types of derogatory information which create a question as to the individual's eligibility for access authorization include, but are not limited to, cases in which the individual has:

1. Committed, prepared or attempted to commit, or aided, abetted or conspired with another to commit or attempt to commit any act of sabotage, espionage, treason, or sedition.

2. Knowingly established or continued a sympathetic association with a saboteur, spy, traitor, seditionist, anarchist, or revolutionist, espionage agent, or representative of a foreign nation whose interests are inimical to the interests of the United States, or with any person advocating the use of force or violence to overthrow the Government of the United States by unconstitutional means.

3. Knowingly held membership in or had a knowing affiliation with, or has taken action which evidences a sympathetic association with the intent of furthering the aims of, or adherence to, and active participation in any foreign or domestic organization, association, movement, group or combination of persons which advocates or practices the commission of acts of force or violence to prevent others from exercising their rights under the Constitution or Laws of the United States or any state or subdivision thereof by unlawful means.

4. Publicly or privately advocates, or participates in the activities of a group or organization, which has as its goal, revolution by force or violence to overthrow the Government of the United States or the alteration of the form of Government of the United States by unconstitutional means with the knowledge that it will further those goals.

5. Parent(s), brother(s), sister(s), spouse, or offspring residing in a nation whose interests may be inimical to the interests of the United States, or in satellites or occupied areas thereof (to be evaluated in the light of the risk that pressure applied through such relatives could force the individual to act contrary to national security).

6. Has deliberately misrepresented, falsified, or omitted significant information from a Personnel Security Questionaire, a personnel qualifications statement, or a personnel security interview.

7. Has failed to protect classified information, or safeguard special nuclear material; or has willfully violated or disregarded se-
curity or safeguards regulations to a degree which would endanger the common defense and security or has intentionally disclosed classified information to a person unauthorized to receive such information.

(8) Has an illness or mental condition of a nature which in the opinion of competent medical authority causes or may cause, significant defect in the judgment or reliability of the individual, or has refused to be examined by a psychiatrist.

(9) Has refused to testify before a Congressional Committee, Federal or state court, or Federal administrative body, regarding charges relevant to eligibility for DOE access authorization.

(10) Is a user of alcohol habitually to excess, or has been such without adequate evidence of rehabilitation or reformation.

(11) Has used, trafficked in, sold, transferred or possessed a drug or other substance listed in the schedule of Controlled Substances established pursuant to section 202 of the Controlled Substances Act of 1970 (such as amphetamines, barbiturates, narcotics, etc.) except as prescribed or administered by a physician licensed to dispense drugs in the practice of medicine, without adequate evidence of rehabilitation or reformation.

(12) Has engaged in any unusual conduct or is subject to any circumstances which tend to show that the individual is not honest, reliable, or trustworthy, and there is no adequate evidence of rehabilitation or reformation; or which furnishes reason to believe that the individual may be subject to coercion, influence, or pressure which may cause the individual to act contrary to the best interests of the national security. Such conduct or circumstances include but are not limited to sexual activity, demonstrated financial irresponsibility or notoriously disgraceful conduct.