

DATE: December 31, 2001

In Re:

SSN: -----

Applicant for Security Clearance

ISCR Case No. 01-07134

DECISION OF ADMINISTRATIVE JUDGE

JEROME H. SILBER

APPEARANCES

FOR GOVERNMENT

William S, Field, Esq., Department Counsel

FOR APPLICANT

Pro Se

SYNOPSIS

Deliberately and deceptively charging personal purchases twice from a wholesaler to the account of a former employer, using a false name, was classified as misdemeanor thefts. Little extenuating or mitigating evidence was offered to substantiate a claim that the conduct was aberrational. Clearance is denied.

STATEMENT OF THE CASE

On September 17, 2001, the Defense Office of Hearings and Appeals (DOHA) pursuant to Executive Order 10865, as amended, and Department of Defense Directive 5220.6, dated January 2, 1992 (Directive), issued a Statement of Reasons (SOR) to the Applicant which detailed reasons why DOHA could not make the preliminary affirmative finding that it is clearly consistent with the national interest to grant or continue a security clearance for the Applicant, and recommended referral to an Administrative Judge to determine whether a clearance should be granted, continued, denied, or revoked. In a written statement, dated September 26, 2001, and notarized on September 29, 2001, the Applicant responded to the allegations set forth in the SOR and elected to have his case decided on a written record, in lieu of a hearing.

The Applicant received a complete copy of the file of relevant material (FORM) on October 16, 2001, and received an opportunity to file objections and submit material in refutation, extenuation, or mitigation. The Applicant elected not to respond to the FORM within the requisite 30 days, *i.e.*, on or before November 15, 2001.. The record in this case closed on November 15, 2001. The undersigned Administrative Judge received the case assignment on December 19, 2001.

FINDINGS OF FACT

The Statement of Reasons (SOR) consisted of allegations predicated on the following two guidelines: paragraph 1, Guideline E (personal conduct), and paragraph 3, Guideline J (criminal conduct). The undersigned Administrative Judge completely and thoroughly reviewed the evidence in the record, and upon due consideration of the same, makes the following Findings of Fact:

The Applicant is a 59-year-old assistant systems administrator employed by a U.S. Government contractor since March 27, 2000. The Applicant seeks to obtain a personnel security clearance.

The Applicant was born abroad and naturalized at age 19 in July 1961. He served in the U.S. Navy from 1961 to 1964 and was discharged as an E-4. A year later he married a U.S.-naturalized woman; the couple has two children, ages 35 and 31. Shortly after his marriage the Applicant began 27 years of service as a U.S. postal employee. After his voluntary retirement from the postal service in 1992, he had a series of jobs, each lasting 21 months or less. He then got a job with Company #1 in November 1997 working in the area of cabling and personal computer support. Because of a job disagreement, he gave his employer two weeks' notice and left that job at the end of April 1999. The Applicant then was employed in two successive jobs in November 1999 through the first week of January 2000. After a period of unemployment lasting less than three months, he was hired by his present employer on March 27, 2000. FORM items 4 and 5.

About the first week of March 2000, and before he was hired by his present employer, the Applicant entered a wholesale computer supply store and purchased some network support items. He was wearing a shirt with the name of Company #1 on it and charged his purchases to that company's account with the wholesale computer supply store using a false name. On March 24, 2000, the Applicant again purchased some more network support items from the same store while wearing the same shirt, using the same false name, and charging them again to Company #1's account. Three days later the Applicant was hired by his present employer.

On March 31, 2001, the Applicant entered the same wholesale computer supply store and attempted to purchase more network support items using the same *modus operandi*. Because Company #1 had rejected the purchases made by the Applicant earlier that month, the employees of the wholesale computer supply store stalled the Applicant and called the police. ⁽¹⁾ The police investigated the situation as a possible case of theft by fraud but no charges were made because the wholesale vendor was satisfied by the immediate cash payment of \$983.87 by the Applicant for the items previously purchased by him. FORM item 6. ⁽²⁾

POLICIES

Enclosure 2 of the Directive (32 C.F.R. part 154 appendix H) sets forth adjudicative guidelines which must be considered in evaluating an individual's security eligibility. The guidelines are divided into those that may be considered in determining whether to deny or revoke a clearance (Disqualifying Conditions or DC) and those that may be considered in determining whether to grant or continue an individual's access to classified information (Mitigating Conditions or MC). In evaluating this case, relevant adjudicative guidelines as set forth below have been carefully considered as the most pertinent to the facts of this particular case.

The guidelines, disqualifying conditions, and mitigating conditions most pertinent to an evaluation of the facts of this case are:

GUIDELINE E - PERSONAL CONDUCT

Conduct involving questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations could indicate that the person may not properly safeguard classified information.

Conditions that could raise a security concern and may be disqualifying also include:

[5th] A pattern of dishonesty or rule violations, including violation of any written or recorded agreement made between the individual and the agency;

Conditions that could mitigate security concerns include:

None applicable.

GUIDELINE J - CRIMINAL CONDUCT

A history or pattern of criminal activity creates doubt about a person's judgment, reliability and trustworthiness.

Conditions that could raise a security concern and may be disqualifying include:

- a. . . . criminal conduct, regardless of whether the person was formally charged;
- b. A single serious crime or multiple lesser offenses.

Conditions that could mitigate security concerns include:

None applicable.

The Directive also requires the undersigned to consider, as appropriate, the factors enumerated in Section 6.3:

- a. Nature and seriousness of the conduct and surrounding circumstances.
- b. Frequency and recency of the conduct.
- c. Age of the applicant.
- d. Motivation of the applicant, and the extent to which the conduct was negligent, willful, voluntary, or undertaken with knowledge of the consequences involved.
- e. Absence or presence of rehabilitation.
- f. Probability that the circumstances or conduct will continue or recur in the future.

Enclosure 2 to the Directive provides that the adjudicator should consider the following factors:

The nature, extent, and seriousness of the conduct

The circumstances surrounding the conduct, to include knowledge-able participation

The frequency and recency of the conduct

The individual's age and maturity at the time of the conduct

The voluntariness of participation

The presence or absence of rehabilitation and other pertinent behavioral changes

The motivation for the conduct

The potential for pressure, coercion, exploitation, or duress

The likelihood of continuation or recurrence

Under the provisions of Executive Order 10865, as amended, and the Directive, a decision to grant or continue an applicant's security clearance may be made only upon an affirmative finding that to do so is clearly consistent with the national interest. In reaching the fair and impartial overall common sense determination required, the Administrative Judge may draw only those inferences and conclusions that have a reasonable and logical basis in the evidence of record. Determinations under the Directive include consideration of the risk that an applicant may deliberately or inadvertently fail to safeguard properly classified information as that term is defined and established under Executive Order 12958, effective on October 14, 1995.

Initially, the Government has the burden of proving controverted facts alleged in the Statement of Reasons. The United States Supreme Court has said:

"It is difficult to see how the Board would be able to review security-clearance determinations under a preponderance of the evidence standard without departing from the 'clearly consistent with the interests of the national security' test. The clearly consistent standard indicates that security-clearance determinations should err, if they must, on the side of denials. Placing the burden on the Government to support the denial [of a security clearance] by a preponderance of the evidence would inevitably shift the emphasis and involve the Board in second-guessing the agency's national security determinations."

Dept. of the Navy v. Egan, 484 U.S. 518, 531 (1988). This Administrative Judge understands that Supreme Court guidance in its context to go to the minimum *quantum* of the admissible evidence that must be adduced by the Government in these proceedings to make its case, that is, substantial evidence but something less than a preponderance of the evidence--rather than as an indication of the Court's tolerance for error below. [\(3\)](#)

The burden of going forward with the evidence then shifts to the applicant for the purpose of establishing his or her security eligibility through evidence of refutation, extenuation or mitigation of the Government's case or through evidence of affirmative defenses. Assuming the Government's case is not refuted, and further assuming it can reasonably be inferred from the facts proven that an applicant might deliberately or inadvertently fail to safeguard properly classified information, the applicant has a heavy burden of persuasion to demonstrate he or she is nonetheless eligible to hold a security clearance. [\(4\)](#)

CONCLUSIONS

Having considered the evidence of record in light of the appropriate legal precepts and factors, the undersigned concludes that the Government established its case with regard to Guidelines E and J.

The Applicant admits the facts alleged in SOR ¶ 1.a., merely correcting the alleged date when the police were called to the wholesale computer supply store, and accepts the consequences of his actions. He claims that the March 2000 "incident" is not representative of his normal conduct. He denies, however, that he has a history of criminal activity and asks that "the one regrettable incident" not be viewed as a "pattern" of criminal activity. FORM item 3.

The evidence shows that the Applicant twice charged his purchases by deception to his former employer, not just once, and that he tried to do so a third time. That is a "history" of criminal conduct, and could be viewed as well as a pattern. This falls within the scope of DC #a under Guideline J, which is identified on page 4 *supra*. The Applicant admits that his conduct in March 2000 constituted "violations" of the state criminal code defining theft (FORM item 7). That code classifies his actions as misdemeanors. These multiple lesser offenses fall within the scope of DC #b.

The Applicant was able to escape prosecution for his actions by paying the wholesale price of the items he purchased although it is clear inference that, not being a current employee of Company #1, he was not entitled to such reduced prices. His claim that he intended to call a particular employee of his former employer and reimburse the company is not given much weight since he allowed some three weeks to elapse without doing so--even though he claimed he was aware of the firm's billing cycle. That he *deliberately* made those deceptive purchases is shown by not simply his wearing a Company #1 shirt but, more convincingly, his charging the purchases to a false name. The Applicant was misusing the firm's creditworthiness rather than his own. Those deceptive purchases constitute a pattern of dishonesty, falling within the scope of DC #5 under Guideline E, which is also identified on page 4 *supra*. The Applicant has not submitted evidence that his actions in March 2000 were aberrational, nor did he submit corroboration of his claim that he has an impeccable work record with his present employer. [\(5\)](#) Therefore, SOR ¶ 1 (personal conduct) and SOR ¶ 2 (criminal conduct) are concluded adversely to the Applicant.

Each clearance decision is required to take into consideration pertinent factors set forth in Section 6.3 of the Directive and in the adjudicative process discussion at enclosure 2 to the Directive. These factors are identified on pages 4-5 *supra*. The nature of the Applicant's conduct was serious. Its recency, his motivation, and his age at the time all weigh against him. The evidence does not support a prediction that the improper conduct will be unlikely to recur in the future.

FORMAL FINDINGS

Formal findings as required by Enclosure 1 of the Directive (see paragraph (7) of section 3 of Executive Order 10865, as amended) and the additional procedural guidance contained in item 25 of Enclosure 3 of the Directive are:

Paragraph 1. Guideline E: AGAINST APPLICANT

Subparagraph 1.a.: Against Applicant

Paragraph 2. Guideline J: AGAINST APPLICANT

Subparagraph 2.a.: Against Applicant

DECISION

In light of all the circumstances presented by the record in this case, it is the determination of the undersigned that it is not clearly consistent with the national interest to grant or continue a security clearance for the Applicant.

Jerome H. Silber

Administrative Judge

1. The Applicant told the police at the wholesale computer supply store on March 31, 2001, that he knew the billing cycle of Company #1 and that it was common practice for its employees to charge their personal purchases to Company #1 and then pay that firm for the charges. He also told the police that he had intended to advise a particular employee of Company #1 about his purchases and reimburse the company. The police then checked with the particular employee named by the Applicant, who denied that there was such a common practice and said that she did not and would not have given the Applicant consent to make his purchases. FORM item 6.

2. The Applicant signed his security clearance application (SF-86) on April 5, 2000. That SF-86 denied that he had any charges pending against him. FORM item 4.

3. The rule has been restated as requiring "that security clearances should be revoked [*sic*] if doing so is consistent with the national interest;" *Doe v. Schachter*, 804 F. Supp. 53, 62 (N.D.Cal. 1992). *Cf.* with regard to the *quantum* of evidence the DOHA Appeal Board analysis in DISCR OSD Case No. 90-1054 (July 20, 1992) at pages 3-5, and DOHA Case No. 94-0966 (July 21, 1995) at pages 3-4. The Directive establishes the following standard of review:

[Whether the] Administrative Judge's findings of fact are supported by such relevant evidence as a reasonable mind might accept as adequate to support a conclusion in light of all the contrary evidence in the same record. In making this review, the [DOHA] Appeal Board shall give deference to the credibility determinations of the Administrative Judge.

Item 32.a. of the Additional Procedural Guidance (Enclosure 3 to the Directive). See also 5 U.S.C. §556(d).

4. While the Government has the burden of proving controverted facts, the Applicant has the ultimate burden of persuasion as to obtaining a favorable clearance decision. Items 14 and 15 of the Additional Procedural Guidance (Enclosure 3 to the Directive).

5. The Applicant was caught by the wholesale computer supply store and investigated by the police on March 31, 2000, four days after he was hired and six days before he signed his SF-86 application for a security clearance. He does not seem to understand that his actions in March 2000 are significantly related to his work record.