DATE: January 9, 2004

In Re:

SSN: ----------

Applicant for Security Clearance

ISCR Case No. 02-18445

DECISION OF ADMINISTRATIVE JUDGE

ROGER E. WILLMETH

APPEARANCES

FOR GOVERNMENT

Rita C. O'Brien, Department Counsel

FOR APPLICANT

Pro Se

SYNOPSIS

The record fails to establish Applicant's untrustworthiness based on his termination by a former employer. Applicant disclosed that he had been "fired" on his security clearance application. He was terminated for violating company policy by using a software program that allegedly made the company's firewall vulnerable. However, the record fails to show that he knew or should have known that the software he used was prohibited or that it actually threatened his company's firewall. Under these circumstances, a single rule violation on the part of Applicant does not establish a disqualifying condition under Guideline E. Clearance is granted.

STATEMENT OF THE CASE

On February 21, 2003, the Defense Office of Hearings and Appeals (DOHA), pursuant to the applicable Executive Order[(1)] and Department of Defense Directive,[(2)] issued a Statement Reasons (SOR) to Applicant. The SOR details security concerns under Guideline E (Personal Conduct). The SOR states that DOHA was unable to find that it is clearly consistent with the national interest to grant him access to classified information and recommends that his case be submitted to an Administrative Judge.

On March 28, 2003, DOHA received a response to the SOR from Applicant in which he requested a decision without a hearing. On September 5, 2003, Applicant submitted comments on the File of Relevant Material (FORM). The case was assigned to me on October 24, 2003.

FINDINGS OF FACT

Having thoroughly considered the evidence in the record, including Applicant's admission to SOR ¶ 1.a, I make the following findings of fact:

Applicant is a 34-year-old field service representative employed by a defense contractor. He is seeking a security

clearance.

On October 23, 1995 Applicant became employed as a customer care consultant by an internet service provider. On October 17, 2001, Applicant's employer terminated him for violating a company policy by using a software program.[(3)]

On March 25, 2002, Applicant submitted a security clearance application (SF 86). In response to question 20 concerning his employment record, Applicant acknowledged he had been "fired" from his prior job. He remarked, "I was released for minor policy violation that was selectively enforced for the purpose of weeding out senior employees."[(4)]

POLICIES

Department Counsel is responsible for presenting witnesses and other evidence to establish facts alleged in the SOR that have been controverted. Directive E3.1.14. The applicant is responsible for presenting witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by the applicant or proven by Department Counsel, and has the ultimate burden of persuasion as to obtaining a favorable clearance decision. Directive E3.1.15.

Eligibility for access to classified information is predicated upon an individual meeting adjudicative guidelines discussed in Enclosure 2 of the Directive. An evaluation of whether an applicant meets these guidelines includes the consideration of a number of variables known as the "whole person concept." Available, reliable information about the person, past and present, favorable and unfavorable, should be considered in reaching a decision. This assessment should include the following factors: (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 individual's age and maturity at the time of the conduct; (5) the voluntariness of participation; (6) the presence or absence of rehabilitation and other pertinent behavioral changes; (7) the motivation for the conduct; (8) the potential for pressure, coercion, exploitation, or duress; and (9) the likelihood of continuation or recurrence. Any doubt as to whether access to classified information is clearly consistent with national security will be resolved in favor of national security. Directive E2.2.2.

Enclosure 2 provides conditions for each guideline that could raise a concern and may be disqualifying, as well as further conditions that could mitigate a concern and support granting a clearance. The following guidelines are applicable to this case.

Guideline E: Personal Conduct

The concern under Guideline E is 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 under Guideline E include E2.A5.1.2.5 (Disqualifying Condition 5). Disqualifying Condition 5 addresses a pattern of dishonesty or rule violations, including violation of any written or recorded agreement made between the individual and the agency.

CONCLUSIONS

As Department Counsel acknowledges, the Government has the burden of proving controverted facts. Directive E3.1.14. The SOR's lone allegation is that Applicant was terminated from his previous employment for "violating company policy by using a software program which made the company's firewall vulnerable." In his security clearance application, Applicant candidly admitted that he was "fired" from his previous employment. He further remarked that it was for a "minor policy violation that was selectively enforced for the purpose of weeding out senior employees."[(5)] Applicant adamantly denies that he knew the use of the software was prohibited or that the program he used actually put his former company's network at risk.

It cannot be determined from the evidence in the FORM the specific policy that Applicant violated. There is also no evidence in the FORM to establish that Applicant was aware or should have known of the policy, or that Applicant's conduct made his former company's firewall vulnerable. Applicant states the software that he utilized did not have such

an effect and there is no evidence in the FORM to rebut this.

Although broader in scope so as to encompass other conduct that may be disqualifying, the majority of Guideline E cases are concerned with whether an applicant has engaged in deliberate omission, concealment, or falsification of relevant and material information in connection with a security clearance application. This has no application to Applicant, who has been forthright about being "fired" by his last employer. To the extent that rule violations, such as Applicant's, are addressed under Guideline E, Disqualifying Condition 5 specifies "a pattern of dishonesty or rule violations." The FORM merely reveals a single rule violation on the part of Applicant. A single rule violation fails to establish Disqualifying Condition 5. ISCR Case No. 99-0040 (October 1, 1999) at 2. Applicant's lone violation of a policy fails to establish a disqualifying condition under Guideline E.[(6)]

Applicant may have violated his former company's policy on one occasion by the use of software. However, this is insufficient to demonstrate untrustworthy conduct on his part when there is no showing that he was aware or should have known of the policy, or that he knew such use threatened the company's firewall. Therefore, I find in favor of Applicant.

FORMAL FINDINGS

Formal findings, as required by section E3.1.25 of Enclosure 3 of the Directive, are as follows:

Paragraph 1. Guideline E: FOR APPLICANT

Subparagraph 1.a: For Applicant

DECISION

In light of the evidence of record in this case, it is clearly consistent with the national interest to grant or continue a security clearance for Applicant.

Signed

Roger E. Willmeth

Administrative Judge

1. Executive Order 10865, *Safeguarding Classified Information Within Industry*, dated February 20, 1960, as amended.

2. Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (Directive), dated January 2, 1992, as amended and modified.

3. Item 4 at 1.

4. Item 3 at 5.

5. Item 3 at 5.

6. The alleged misconduct in this case is specifically addressed by Guideline M, pertaining to misuse of information technology systems. Disqualifying Condition 4 under Guideline M addresses the introduction of hardware, software or media into any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines, or regulations (Disqualifying Condition 4). However, the evidence in the FORM fails to establish the specific policy that Applicant violated. Moreover, a disqualifying condition under Guideline M may be mitigated when the conduct was unintentional or inadvertent (Mitigating Condition 2) or the misuse was an isolated event (Mitigating Condition 4). There is evidence in the FORM that would support both of these mitigating conditions. Applicant describes his understanding of the type of online activity his former company prohibited and states he was not aware that it included what he did. There is no evidence in the FORM to rebut him. There is also no evidence in the form that

reveals any other misuse on Applicant's part.