DATE: July 25, 2003

In Re:

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

Applicant for Security Clearance

ISCR Case No. 01-07626

DECISION OF ADMINISTRATIVE JUDGE

RICHARD A. CEFOLA

APPEARANCES

FOR GOVERNMENT

Jennifer I. Campbell, Esquire, Department Counsel

FOR APPLICANT

Pro Se

SYNOPSIS

The Applicant's security clearance was revoked in May of 1988, a fact that he acknowledged by way of correspondence in July of 1988, in September of 1988, and in April of 1989. In October of 1995, however, the Applicant denied that his clearance had ever been "denied, suspended or revoked," when he executed his Personnel Security Questionnaire (PSQ). This lack of candor, coupled with the fact that he admittedly improperly copied computer software from 1990~1999 and still uses that software, brings into question the Applicant's trustworthiness. No mitigation has been shown. Clearance is denied.

STATEMENT OF THE CASE

On February 24, 2003, the Defense Office of Hearings and Appeals (DOHA), pursuant to Executive Order 10865 and Department of Defense Directive 5220.6 (Directive), dated January 2, 1992, issued a Statement of Reasons (SOR) to the Applicant, which detailed reasons why DOHA could not make the preliminary affirmative finding under the Directive 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 denied or revoked.

Applicant filed an Answer to the SOR on March 25, 2003.

Applicant elected to have this case determined on a written record in lieu of a hearing. Department Counsel submitted the Government's File of Relevant aterial (FORM) on May 15, 2003. Applicant was instructed to submit objections or information in rebuttal, extenuation or mitigation within 30 days of receipt of the FORM. Applicant received his copy on May 29, 2003, and submitted nothing in reply. The case was received by the undersigned for resolution on July 10, 2003. The issues raised here are whether the Applicant's personal conduct and related misuse of information technology militate against the granting of a security clearance. [The Applicant denies all of the allegations, except for allegation 1.c., as it relates to the improper copying of computer software, under personal conduct.]

FINDINGS OF FACT

The following Findings of Fact are based on Applicant's Answer to the SOR, and the File of Relevant Material. The Applicant is 57 years of age, and is employed by a defense contractor who seeks a security clearance on behalf of the Applicant. After a complete and thorough review of the evidence in the record, and upon due consideration of the same, I make the following additional findings of fact.

Guideline E - Personal Conduct & Guideline M - Misuse of Information Technology

1.a. and 1.d. In May of 1988, the Applicant's security clearance was revoked (Government Exhibit (GX 7). The Applicant acknowledged that his clearance was revoked or that his access to information was denied in correspondence dated July 6, 1988 (GX 7 at page 1), in correspondence dated September 20, 1988 (GX 7 at page 6), again in correspondence dated April 26, 1989 (GX 7 at page 5), and most recently in a sworn statement dated June 10, 1999 (GX 5 at page 12). In October of 1995, however, when executing his PSQ, he answered "No" to the question "Have you ever had a security clearance denied, suspended or revoked" (GX 4 at page 4). I find this to be a knowing and wilful falsification. Furthermore, the Applicant did not come forward and explain his falsification until more than three and a half years later, when he executed the sworn statement (GX 5).

1.b. In June of 1999, the Applicant did admit to "have taken home some . . . [of his employer's] proprietary information over the past several years," but he avers that such conduct was sanctioned by his employer (GX 5 at page 14). The Government has failed to demonstrate otherwise; and as such, this allegation is found for the Applicant.

1.c. and 2.a. The Applicant admittedly copied computer software without the permission or authorization from the software manufacturer from 1990~1999, and he continues to use such software (GX 3 at page 5, and GX 5 at pages 17~18).

Mitigation

The Applicant offers little in the way of mitigation, and only tries to explain away his clear falsification.

POLICIES

Enclosure 2 and Section E.2.2. of the 1992 Directive set forth both policy factors, and conditions that could raise or mitigate a security concern; which must be given binding consideration in making security clearance determinations. The conditions should be followed in every case according to the pertinent criterion, however, the conditions are neither automatically determinative of the decision in any case, nor can they supersede the Administrative Judge's reliance on his own common sense. Because each security clearance case presents its own unique facts and circumstances, it should not be assumed that these conditions exhaust the realm of human experience, or apply equally in every case. Conditions most pertinent to evaluation of this case are:

Personal Conduct

Conditions that could raise a security concern:

2. The deliberate omission, concealment, or falsification of relevant and material facts from any personnel security questionnaire . . . ;

5. A pattern of dishonesty or rule violations . . . ;

Conditions that could mitigate security concerns:

None

Misuse of Information Technology Systems

Condition that could raise a security concern:

3. Removal (or use) . . . of software . . . without authorization;

Conditions that could mitigate security concerns:

None

As set forth in the Directive, each clearance decision must be a fair and impartial common sense determination based upon consideration of all the relevant and material information and the pertinent criteria and adjudication policy in enclosure 2, including as appropriate:

a. Nature, extent, and seriousness of the conduct, and surrounding circumstances.

b. Frequency and recency of the conduct.

c. Age and maturity 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 consequence involved.

e. Absence or presence of rehabilitation.

f. Probability that circumstances or conduct will continue or recur in the future."

The Administrative Judge, however, can only draw those inferences or conclusions that have a reasonable and logical basis in the evidence of record. The Judge cannot draw inferences or conclusions based on evidence that are speculative or conjectural in nature.

The Government must make out a case under Guidelines E (personal conduct), and M (misuse of information technology systems); which establishes doubt about a person's judgment, reliability and trustworthiness. While a rational connection, or nexus, must be shown between an applicant's adverse conduct and his ability to effectively safeguard classified information, with respect to sufficiency of proof of a rational connection, objective or direct evidence is not required.

Then, the Applicant must remove that doubt with substantial evidence in refutation, explanation, mitigation or extenuation, which demonstrates that the past adverse conduct is unlikely to be repeated, and that the Applicant presently qualifies for a security clearance.

The Government must be able to place a high degree of confidence in a security clearance holder to abide by all security rules and regulations at all times and in all places. If an applicant has demonstrated a lack of respect for rules, there then exists the possibility that an applicant may demonstrate the same attitude towards security rules and regulations.

CONCLUSIONS

The Applicant was clearly less than candid with the Government when he executed his PSQ in October of 1995. His access to classified information had been denied and his clearance had been revoked six years earlier in May of 1988. It is clear from the intervening correspondence that he was aware of the prior demise of his security clearance, but in his answer he tries to explain away his clear falsification, averring that his access was not really denied nor his clearance really revoked. His explanation is not supported by any other evidence, and, in the context of the entire record, I find it to be not credible. This poor exercise of semantics, coupled with the fact he admittedly has copied and still uses computer software he had no authority to copy, further brings into question the Applicant's trustworthiness. His wilful falsification and continued misuse of information technology are clearly of security clearance significance; and as such, Guidelines E and M are therefore found against the Applicant.

FORMAL FINDINGS

Formal Findings required by paragraph 25 of Enclosure 3 of the Directive are:

Paragraph 1: AGAINST THE APPLICANT

a. Against the Applicant.

b. For the Applicant.

c. Against the Applicant.

d. Against the Applicant.

Paragraph 2: AGAINST THE APPLICANT

a. Against the Applicant.

Factual support and reasons for the foregoing are set forth in **FINDINGS OF FACT** and **CONCLUSIONS**, supra.

DECISION

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

Richard A. Cefola

Administrative Judge