DATE: October 16, 2002

In Re:

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

Applicant for Security Clearance

ISCR Case No. 01-16493

DECISION OF ADMINISTRATIVE JUDGE

RICHARD A. CEFOLA

APPEARANCES

FOR GOVERNMENT

Melvin A. Howry, Esquire, Department Counsel

FOR APPLICANT

Alan V. Edmunds, Esquire, Applicant's Counsel

SYNOPSIS

The Applicant complied with his employer's rules, procedures and guidelines in making two intranet connections onto his employer's network. As a result, his subsequent termination by his employer was based upon faulty information. Clearance is granted.

STATEMENT OF THE CASE

On May 15, 2002, 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 the 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 June 13, 2002.

The case was received by the undersigned on August 27, 2002. A notice of hearing was issued on September 3, 2002, and the case was heard on September 30, 2002. The Government submitted documentary evidence. Testimony was taken from the Applicant, who called four witnesses to testify on his behalf. The transcript was received on October 8, 2002. The issues raised here are whether the Applicant's alleged misuse of information technology systems, and related personal conduct, militate against the granting of a security clearance.

FINDINGS OF FACT

The following Findings of Fact are based on Applicant's Answer to the SOR, the documents and the live testimony. The Applicant is 56 years of age, has a high school education, and is employed by a defense contractor who seeks a security clearance on behalf of the Applicant.

Guideline M - Misuse of Information Technology Systems & Personal Conduct

1.a., 1.b. and 2.a. For a number of years prior to August 24, 2000, it had been standard practice for employees of an aerospace employer to make intranet connections onto their employer's network as part of their mission assignment (Transcript (TR) at page 27 lines 1 to 14, at page 52 line 18 to page 53 line 5, and at page 74 line 21 to page 75 line 8). Employees were taught to seize the initiative and to make such connections, on short notice, in support of their mission (*id*). This standard operating procedure (SOP) began to change, however, when the aerospace employer instituted an Information Technology (IT) Department (TR at page 53 line 21 to page 54 line 18, and at page 72 line 17 to page 73 line 8). IT, however, was not very responsive to the immediate needs of their in-house customers (*id*).

On August 24, 2000, the Applicant, relying on the unwritten SOP and unable to get any response for help from IT, made an intranet connection onto his employer's network (TR at page 73 line 20 to page 76 line 1, at page 96 line 10 to page 97 line 20, *see also* Applicant's Exhibit (AppX) E at pages 2~4). He was subsequently told by IT that this intranet connection was not made with their prior approval; and as such, was unauthorized (TR at page 97 lines 21~25, *see also* AppX at pages 2~4). On August 27, 2000, the Applicant, again was required to make an intranet connection. This time, however, he sought out and got the verbal approval of IT (TR at page 71 line 6 to page 72 line 16, at page 81 lines 3~20, at page 87 lines 8~23, and at page 98 line 1 to page 99 line 7, *see also* AppX E at pages 2~4). After the connection was made, however, IT did an about face and declared it to be unauthorized (TR at page 87 line 24 to page 89 line 7, at page 99 lines 8~12, *see also* AppX E at pages 2~4).

As a result of these two alleged "unauthorized" connections, the Applicant was terminated from his employment with the aerospace firm, a firm he had worked for, for 28 years (Government Exhibit (GX) 4). Normally, such an alleged infraction was handled with a simple "warning notice" (TR at page 39 lines 12~25, and at page 60 lines 5~15).

Mitigation

Four former supervisors testified on behalf of the Applicant (TR at page 17 line 9 to page 21 line 9, at page 22 line 9 to page 39 line 25, at page 41 line 12 to page 48 line 2, and at page 49 line 11 to page 62 line 13). They were all most laudatory in their comments as to the Applicant. A retired Air Force Colonel, who was the Applicant's supervisor from 1993~1998, was very upset with the Applicant's termination. He described the head of IT, who at one junction also worked for the witness for "at least five years," as "a weak individual. I would never put him in a leadership or management position . . ." (TR at page 58 lines 13~18).

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:

Misuse of Information Technology Systems

Condition that could raise a security concern:

1. Illegal or unauthorized entry into any information technology system;

Condition that could mitigate security concerns:

2. The conduct was unintentional or inadvertent;

Personal Conduct

Conditions that could raise a security concern:

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 M (misuse of information technology systems), and E (personal conduct); 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 allegedly made two unauthorized intranet connections onto his employer's network. Both connections were made in support of his employer's mission, and he was either following his employer's long standing SOP or had the verbal authorization of IT in support of his actions. The "unauthorized" characterization of his connections, was, at best; a subsequent judgmental call by his employer. All who testified thought the Applicant's actions were prudent and necessary in support of his employer's mission. I can find no knowing unauthorized conduct or rule violation here; and as such, Guidelines M and E are therefore found for the Applicant.

FORMAL FINDINGS

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

Paragraph 1: FOR THE APPLICANT

a. For the Applicant.

b. For the Applicant.

Paragraph 2: FOR THE APPLICANT

a. For 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 clearly consistent with the national interest to grant or continue a security clearance for the Applicant.

Richard A. Cefola

Administrative Judge