DATE: July 18, 2006

In Re:

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

Applicant for Security Clearance

ISCR Case No. 04-11384

DECISION OF ADMINISTRATIVE JUDGE

JOSEPH TESTAN

APPEARANCES

FOR GOVERNMENT

Fahryn E. Hoffman, Department Counsel

FOR APPLICANT

Pro Se

SYNOPSIS

Applicant's intentional misuse of his employer's computer occurred over a six month period, and resulted in his employer having to refund money it had improperly billed to its customers. Clearance is denied.

STATEMENT OF THE CASE

On September 16, 2005, 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 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 applicant and recommended referral to an Administrative Judge to determine whether clearance should be denied or revoked.

Applicant responded to the SOR in writing on October 4, 2005, and elected to have his case determined on a written record in lieu of a hearing. Department Counsel submitted the Government's written case (FORM) on or about December 16, 2005. Applicant filed a response to the FORM on January 12, 2006. The case was assigned to me on January 25, 2006.

FINDINGS OF FACT

Applicant is a 50 year old employee of a defense contractor. He has worked in the defense industry since at least 1979.

During a period of approximately six months ending in early 2001, applicant used his employer's computer on at least 1,337 occasions to access or attempt to access sexually explicit web sites. His employer estimated that during this time applicant spent about 25% of his work hours engaging in this misconduct. As a result of knowingly violating his company's rules, procedures and guidelines, applicant resigned in lieu of being fired.

At the time he committed the misconduct, applicant's work hours were being billed to his employer's customers.

Following an investigation, the employer concluded that 260 of applicant's work hours had been improperly billed and had to be refunded to the customers.

Applicant accepts full responsibility for his actions, and states he has taken steps to resolve the issues that led to his misconduct.

In 1985, applicant was given a written reprimand for certifying and approving inaccurate start and stop time for his employees. Based on the statement in the written reprimand that "there appears to be no intent on your part to defraud [his defense contractor employer] or its customers," applicant's conduct appears to have been negligent as opposed to intentional (Exhibit 9). Given this fact, and the fact this incident occurred 20 years ago, I find that it has no current security significance.

CONCLUSIONS

The evidence establishes that during a period of approximately six months ending in early 2001, applicant used his company computer to access and attempt to access sexually explicit web sites in violation of his employer's rules, procedures and guidelines. This fact requires application of Guideline M's Disqualifying Condition E2.A13.1.2.3 *(removal (or use) of hardware, software, or media from any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations)* and Guideline E's Disqualifying Condition E2.A5.1.2.5 *(a pattern of dishonesty or rule violations . . .)*.

Applicant does not qualify for any formal mitigating conditions under either guideline. Mitigating Condition E2.A13.1.3.1 does not apply because, although the misuse was not recent, it clearly was significant. Mitigating Condition E2.A13.1.3.2 does not apply because applicant's conduct was intentional. And, Mitigating Condition E2.A13.1.3.4 does not apply because applicant's conduct clearly was not an isolated event.

In reaching a decision in this case, I have considered the fact that applicant has served in the defense industry since at least 1979, and except for the written reprimand he received for a relatively minor incident 20 years ago, this incident of computer-related misconduct appears to be the only incident of misconduct on his part during his entire career. This is certainly a factor in his favor. However, given the facts that applicant's misconduct was intentional and long-running, and the fact that since he knew his hours were being billed to his employer's customers he had to know at some level that he was defrauding his employer's customers, I cannot conclude at the present time that it is clearly consistent with the national interest for applicant to have access to classified information.

FORMAL FINDINGS

GUIDELINE M: AGAINST THE APPLICANT

GUIDELINE E: AGAINST THE APPLICANT

DECISION

In light of all 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 applicant.

_____

Joseph Testan

Administrative Judge