DATE: November 27, 2006

In re:

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

Applicant for Security Clearance

CR Case No. 06-03606

DECISION OF ADMINISTRATIVE JUDGE

SHARI DAM

APPEARANCES

FOR GOVERNMENT

Emilio Jaksetic, Esq., Department Counsel

FOR APPLICANT

Pro Se

SYNOPSIS

Applicant is a 52-year-old electrical engineer, who has worked for federal contractors for the past 20 years and held a security clearance. From approximately October 2002 to August 2003, Applicant used the government computer to access various pornographic and foreign web sites and to download media without authorization. In 2003 he was terminated from a position for his misconduct. He failed to mitigate the security concerns raised by his misuse of information technology systems and personal conduct. Clearance is denied.

STATEMENT OF THE CASE

On May 29, 2001, Applicant submitted a security clearance application (SF86). On July 18, 2006, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) to Applicant, under Executive Order 10865, *Safeguarding Classified Information Within Industry*, as amended, and Department of Defense Directive 5220.6, *Defense Industrial Security Clearance Review Program* (Directive), dated January 2, 1992, as amended. The SOR detailed reasons under Guideline M (Misuse of Information Technology System) and Guideline E (Personal Conduct) why DOHA could not make a preliminary affirmative finding under the Directive that it is clearly consistent with the national interest to grant a security clearance to Applicant. DOHA recommended the case be referred to an administrative judge to determine whether a clearance should be granted.

On August 7, 2006, Applicant filed his Answer, admitted all allegations, and elected to have the case decided on the written record in lieu of a hearing. On August 30, 2006, Department Counsel prepared a File of Relevant Material (FORM), containing ten Items, and mailed it the following day. Applicant had 30 days from receipt of the FORM to file objections and submit material in refutation, extenuation, or mitigation. Applicant received the FORM on September 12, 2006, and submitted additional information within 30 days that consisted of 19 exhibits (AX). Department Counsel did not object to the additional materials. The case was assigned to me on October 25, 2006.

FINDINGS OF FACT

Based on the entire record, including Applicant's admissions in his Answer to the SOR, I make the following findings of fact:

Applicant is 52 years old, married and has two children, ages 19 and 14. He escaped Vietnam as a refugee in May 1975 and came to the United States. He subsequently became a citizen and earned a degree in electrical engineering. (9/24/2006 Letter)

Applicant worked as a system's engineer for a federal contractor from June 1984 until August 2003 when he was terminated for using the company's computer, without authorization, to access various pornographic web sites, dating services, foreign chat rooms, and to download nude pictures and other items unrelated to his job. (Item 5) A company audit indicated that he "hit the access denied page 1,364 times in the month of June 2003 . . . and 4,243 times in July." (*Id.*) Over the course of one month, he spent 84 hours on the internet. (*Id.*) In his answer to the SOR, Applicant admitted he spent almost half of his work hours visiting various sites unrelated to his job from October 2002 until August 2003, in violation of company rules and procedures.

Although Applicant initially denied the misconduct when confronted by his employer on August 19, 2003, he admitted it later that day and sent an email to his supervisor apologizing for his wrongful conduct. He attributed his behavior to stress related to his wife's illness and father's death. He did not intend to violate the company's policy on internet usage. He stated, "I am committed to get the professional help and do whatever necessary to make sure that I will not make this mistake again." (AX 7) He held a security clearance at the time. (Item 5 at 6) Prior to the termination, he received numerous awards and Certificates of Accomplishment from his employer. (AX 3, 4 and 5)

Upon being discharged by his employer, Applicant lost all of his benefits. He appealed that decision to the state's unemployment insurance appeals board. After a hearing the administrative law judge found that Applicant "was not aware that he violated any employer policies. His use of the Internet did not affect his work." (AX 8) In December 2003, the board reinstated his benefits.

Applicant remained unemployed until April 2004 at which time he started his current position with another defense contractor. Over the course of his employment, he has taken several on-line courses in ethics and DoD security awareness issues. (AX 13 and 14) His performance evaluations indicate that he meets his company's expectations. (AX 12)

Applicant's two daughters, lovingly, submitted letters on his behalf. They are aware of his misconduct and remorse. They believe he is an honest man and attribute the problem to a significant amount of family stress. (AX 15) Three of Applicant's colleagues also submitted supportive letters, including one from his security officer. All of them are aware of the situation, but consider him trustworthy and not a security risk. (AX 17-19)

POLICIES

Enclosure 2 of the Directive, *Adjudicative Guidelines for Determining Eligibility for Access to Classified Information,* sets forth criteria, which must be evaluated when determining security clearance eligibility. Within those adjudicative guidelines are factors to consider in denying or revoking an individual's request for access to classified information (Disqualifying Conditions), and factors to consider in granting an individual's request for access to classified information (Mitigating Conditions). By recognizing that individual circumstances of each case are different, the guidelines provide substantive standards to assist an administrative judge in weighing the evidence in order to reach a fair, impartial and common sense decision.

The adjudicative process requires thorough consideration and review of all available, reliable information about the applicant, past and present, favorable and unfavorable, to arrive at a balanced decision. Section E2.2. of Enclosure 2 of the Directive describes the essence of scrutinizing all appropriate variables in a case as the "whole person concept." In evaluating the disqualifying and mitigating conduct an administrative judge should consider: (1) the nature, extent, and seriousness of the conduct; (2) the circumstances surrounding the conduct; (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 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.

Granting an applicant's clearance for access to classified information is based on a high degree of trust and confidence in the individual. Accordingly, decisions under the Directive must include consideration of not only the *actual* risk of disclosure of classified information, but also consideration of any *possible* risk an applicant may deliberately or inadvertently compromise classified information. Any doubt about whether an applicant should be allowed access to classified information must be resolved in favor of protecting classified information. Directive ¶ E2.2.2. The decision to deny an individual a security clearance is not necessarily a judgment about an applicant's loyalty. Exec. Or. 10865, § 7. Instead, it is a determination that an applicant has not met the strict guidelines established by the Department of Defense for issuing a clearance.

Initially, the Government must establish, by substantial evidence, conditions in the personal or professional history of the applicant that disqualify, or may disqualify, the applicant from being eligible for access to classified information. *Departments of the Navy V. Egan,* 484 U.S. 518, 531 (1988). The Directive presumes a rational connection between past proven conduct under any disqualifying conditions and an applicant's present security suitability. *See* ISCR Case No. 95-0611 at 2 (App. Bd. May 2, 1996).

Once the Government establishes a disqualifying condition by substantial evidence, the corresponding burden of rebuttal shifts to the applicant to present evidence in refutation, extenuation, or mitigation sufficient to overcome the position of the government. *See* ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002); Directive ¶ E3.1.15. An applicant "has the ultimate burden of demonstrating that it is clearly consistent with the national interest to grant or continue his clearance." (*Id.*)

Based upon the allegations contained in the SOR and a consideration of the evidence as a whole, the following adjudicative guidelines are pertinent to an evaluation of this case:

Guideline M - Misuse of Information Technology Systems: A security concern may exist when the noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems raises security concerns about an individual's trustworthiness, willingness, and ability to properly protect classified systems, networks, and information. Information Technology Systems include all related equipment used for the communication, transmission, processing, manipulation, and storage of classified or sensitive information.

Guideline E - Personal Conduct: A security concern may exist when 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.

The disqualifying and mitigating conditions, raising either security concerns or mitigating security concerns applicable to this case, are set forth and discussed in the Conclusions section below.

CONCLUSIONS

I have considered all of the facts in evidence and legal standards, including the "whole person" concept, and conclude the following with respect to the allegations set forth in the SOR:

Guideline M: Misuse of Information Technology Systems

The Government established a potential disqualification under Misuse of Information Technology Systems Disqualifying Condition (MIS DC) E2.A13.1.2.4 (*Introduction of hardware, software or media into any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations)* applies. Applicant admitted that from approximately October 2002 until August 2003, he accessed pornographic web sites and downloaded files unrelated to the performance of his job without authorization from his employer, in violation of the company's regulations.

The Government having raised a security concern, the burden shifted to Applicant to mitigate or rebut the allegations. After reviewing all of the Misuse of Information Technology Systems itigating Conditions (MIS MC), in particular, MIS CM E2.A13.1.3.1 *(The misuse was not recent or significant),* MIS MC E2.A13.1.3.2 (*The conduct was*

unintentional or inadvertent), and MIS C E2.A13.1.3.4 *(The misuse was an isolated event),* I concluded none apply. Applicant misused his company's internet from October 2002 until he was caught in August 2003. While his misconduct may not be recent, it was significant in the amount of time he spent engaged in it, and was intentional and repeated; hence, it is not mitigated under E2.A13.1.3.1, E2.A13.1.3.2, or E2.A13.1.3.4. Because the company confronted him with documentation of the misconduct and he did not volunteer the information, MIS MC E2.A13.1.3.5 (*The misuse was followed by a prompt, good faith effort to correct the situation)* cannot apply.

Guideline E: Personal Conduct

The Government established a potential disqualification under Personal Conduct Disqualifying Condition (PC DC) E2.A5.1.2.1 (*Reliable, unfavorable information provided by associates, employers, coworkers, neighbors, and other acquaintances*), and PC DC E2.A5.1.2.5 (*A pattern of dishonesty or rule violations, including violation of any written or recorded agreement made between the individual and the agency*). Applicant's previous employer terminated him after 19 years when they became aware of his unauthorized use of the internet, which spanned ten months and established a pattern of violating company rules. I reviewed all Personal Conduct Mitigating Conditions and concluded none of them are pertinent to the facts in this case, nor do they need to be considered in order to arrive at a final decision. *See* ISCR Case No. 03-21220 (App. Bd. Aug.24., 2005)

The Whole Person Analysis

In addition to the enumerated disqualifying and mitigating conditions, I also considered the evidence in the context of the whole person, including Applicant's 19 years of successful performance with his former employer, years of holding a security clearance without problems, letters from his family and co-workers, in addition to his current performance evaluations and ethics training. I also took into account Applicant's middle age at the time of the incidents, the scope of the misconduct, and a legal finding that he did not know his computer activities were violating company policies, which I find incredible given his position and length of employment. While he is presently exhibiting positive signs of rehabilitation, including deep remorse, I am not persuaded that his conduct since August 2003 is sufficient to mitigate the disqualifications. In his August 2003 letter to the company, he stated he was "committed to get the professional help and do whatever necessary to make sure that I will not make this mistake again." However, he did not present any evidence that he sought professional help or took additional behavioral steps as he asserted. Without objective evidence from a credentialed professional to verify an understanding of his previous reaction to stress and to corroborate behavioral changes, an unblemished record for the past three years does not sufficiently convince me that such conduct could not recur in the future. Hence, he failed to mitigate the security concerns raised by his misuse of information technology systems and personal conduct, as alleged in the SOR. Accordingly, Guidelines M and E are decided against Applicant.

FORMAL FINDINGS

Formal Findings for or against Applicant on the allegations set forth in the SOR, as required by Section E3.1.25 of Enclosure 3 of the Directive, are as follows:

Paragraph 1: Guideline M (Misuse of Information Technology) AGAINST APPLICANT

Subparagraphs 1.a - 1.e: Against Applicant

Paragraph 2: Guideline E (Personal Conduct) AGAINST APPLICANT

Subparagraph 2.a: Against Applicant

DECISION

In light of all the circumstances and evidence presented in this case, it is not clearly consistent with the national interest to grant a security clearance to Applicant. Clearance is denied.

Shari Dam

Administrative Judge