DATE: February 24, 2004

In Re:

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

Applicant for Security Clearance

ISCR Case No. 02-23437

DECISION OF ADMINISTRATIVE JUDGE

CHARLES D. ABLARD

APPEARANCES

FOR GOVERNMENT

Jennifer Campbell, Esq., Department Counsel

FOR APPLICANT

Daniel D. Sorenson, Esq.

SYNOPSIS

Applicant is a 42-year-old employee of a defense contractor working as a senior engineer.

Applicant has held a security clearance for the past 16 years while he was employed by other defense contractors and the Navy. Applicant was discharged in 1991 by a former employer for use of the internet to view pornography on two occasions in violation of company computer policy. Applicant has an unblemished outstanding record of employment both before and after the termination. He has received counseling after his discharge. Clearance is granted.

STATEMENT OF THE CASE

On August 11, 2003, the Defense Office of Hearings and Appeals (DOHA) pursuant to Executive Order 10865, *Safeguarding Information Within Industry,* as amended and modified, and Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (Directive), dated January 2, 1992, as amended and modified, 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. DOHA recommended the case be referred to an administrative judge to determine whether a clearance should be granted, continued, denied, or revoked.

In a sworn written statement, dated September 5, 2003, Applicant responded to the allegations set forth in the SOR, and requested a hearing. The case was assigned to me on December 3, 2003. A hearing was held on December 12, 2003. The Government and the Applicant each introduced three exhibits at the hearing. All exhibits were accepted into evidence. The transcript was received on December 31, 2003.

FINDINGS OF FACT

Applicant has admitted the specific factual allegation in the SOR relating to the internet violation but denied the implications of the admission. The admission is incorporated herein as a finding of fact. After a complete review of the

evidence in the record and upon due consideration of the record the following additional findings of fact are made.

Applicant is a 42-year-old employee of a defense contractor working as a senior engineer.

Applicant has held a security clearance for the past 16 years while he was employed by other defense contractors and as a federal civil servant for the Navy.

Applicant was discharged in 1991 by a former employer for improper use of the internet to view pornography in violation of company computer policy. (Exh. 2) He had worked there four months and accessed the prohibited material on two occasions. The former employer was a manufacturer and vendor of medical equipment with no access to classified information.

Applicant is married with four children ranging in age from six to 15. (TR. 58) He sought marital counseling from a family therapist and from his church after his discharge by his former employer. (TR. 60) Testimony was received at the hearing from the therapist who concluded that Applicant had no family or social problems that required further treatment and that he had terminated his services to him as he no longer needed assistance. (TR. 65)

Applicant is successful in his present employment where he has worked since 2001. He has been given an extraordinary performance rating and cash awards for his services to the company. (Exh. A, B, and C)

POLICIES

"[N]o one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988). As Commander-in-Chief, the President has "the authority to control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to occupy a position that will give that person access to such information." *Id.* at 527.

An evaluation of whether the applicant meets the security guidelines includes consideration of the following factors: (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. Directive, ¶ E2.2.1. Security clearances are granted only when "it is clearly consistent with the national interest to do so." Executive Order No. 10865 § 2. *See* Executive Order No. 12968 § 3.1(b).

Initially, the Government must establish, by something less than a preponderance of the evidence, that conditions exist in the personal or professional history of the applicant which disqualify, or may disqualify, the applicant from being eligible for access to classified information. *See Egan*, 484 U.S. at 531. The Applicant then bears the burden of demonstrating that it is clearly consistent with the national interest to grant or continue the Applicant's clearance. "Any doubt as to whether access to classified information is clearly consistent with national security will be resolved in favor of the national security." Directive, ¶ E2.2.2. "[S]ecurity clearance determinations should err, if they must, on the side of denials." *Egan*, 484 U.S. at 531. *See* Executive Order No. 12968 § 3.1(b)

Misuse of Information Technology Systems under Guideline M is raised regarding noncompliance with rules and regulations regarding use of an information technology system. The concern expressed is that noncompliance with rules or regulations pertaining to information technology systems may raise security concerns about an individual's trustworthiness, willingness, and ability to properly protect classified systems, networks and information. The Guideline goes on to define Information Technology Systems to include all equipment used for the communication, transmission, processing, manipulation, and storage of classified or sensitive information. (E2.A13.1.1.) Conditions that could raise a security concern and may be disqualifying include illegal or unauthorized entry into any information technology system. (E2.A13.1.2.1.) Conditions that could mitigate the security concerns include the fact that the misuse was an isolated event. (E2.A13.1.3.4.)

Personal Conduct (DC) 5 under Guideline E is raised in that the misuse of an Information Technology System shows questionable judgement or unwillingness to comply with rules and regulations that could indicate that the person may

not properly safeguard classified information. (E2.A5.1.1.) Applicable mitigating conditions might include the fact that the individual has taken positive steps to significantly reduce kor eliminate vulnerability to coercion, exploitation, or duress. (E2.A5.1.3.5.)

CONCLUSIONS

Upon consideration of all the facts in evidence, and after application of all appropriate legal precepts, factors, and conditions, I conclude the following with respect to all allegations set forth in the SOR.

Based on the evidence of record, including Applicant's admissions, the Government has stated reasons to deny him a security clearance based on misuse of information technology systems, and personal conduct. Having established the facts in support of such reasons, the Applicant has the burden to establish security suitability through evidence which refutes, mitigates, or extenuates the disqualification and demonstrates that it is clearly consistent with the national interest to grant a security clearance. ISCR Case No. 99-0424 (App. Bd. Feb. 8, 2001)

While there is no evidence that the computer Applicant accessed in violation of his former employer's rules contained classified information and likely did not, the employer considered that the information was sensitive and had very specific rules about use of the system including the receipt and viewing of obscene materials. (Exh. 2 pp. 14 and 15) Thus, the test of whether the system was covered by the Guideline was met. ISCR Case No. 99-0554 (App. Bd. July 24, 2000)

Applicant has acknowledged that he erred in his conduct and the ensuing termination brought home to him that he needed counseling for his family life to ensure that he continued to have a successful marriage. Applicant acknowledged that he had on a few occasions viewed websites containing obscene materials on his home computer but after his counseling now realizes that it has an adverse affect on his behavior and refuses to do so now thus lessening the likelihood of vulnerability to exploitation.

Applicant's long record of service to the defense industry and the Navy overrides his two transgressions in violation of a private employer's policy that occurred four years ago. Having observed Applicant's demeanor, I find him credible and sincere in taking responsibility for his conduct and his efforts to avoid future errors in judgment. I find that the misuse of an information technology system was an isolated event and is not at this time pertinent to a determination of security worthiness. Applicant has divulged all relevant information to his ecclesiastical counselor and his wife who attended the entire hearing. Mitigating conditions cited above for both Guidelines M and E are applicable.

In all adjudications the protection of our national security is of paramount concern. Persons who have access to classified information have an overriding responsibility for the security concerns of the nation. The objective of the security clearance process is the fair-minded, commonsense assessment of a person's trustworthiness and fitness for access to classified information.

The "whole person" concept recognizes that we should view a person by the totality of their acts and omissions. Each case must be judged on its own merits taking into consideration all relevant circumstances, and applying sound judgment, mature thinking, and careful analysis.

After considering all the evidence in its totality and as an integrated whole to focus on the whole person of Applicant, I conclude that the Applicant is a trustworthy and reliable person whose record of conduct and employment justifies a finding that it is clearly consistent with the national interest to grant a security clearance to him.

FORMAL FINDINGS

Formal Findings as required by Section E3.1.25 of Enclosure 3 of the Directive are hereby rendered as follows:

Paragraph l Guideline M: FOR APPLICANT

Subparagraph 1.a.: For Applicant

Paragraph 2 Guideline E: FOR APPLICANT

Subparagraph 2.a.: For Applicant

DECISION

In light of all the circumstances and facts presented by the record in this case, it is clearly consistent with the national interest to grant a security clearance for Applicant.

Charles D. Ablard

Administrative Judge