DATE: February 15, 2002

In Re:

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

Applicant for Security Clearance

CR Case No. 01-03107

DECISION OF ADMINISTRATIVE JUDGE

APPEARANCES

FOR GOVERNMENT

Melvin A. Howry, Esquire, Department Counsel

FOR APPLICANT

Andrew Skowronek, Esquire

STATEMENT OF THE CASE

On April 25, 2001, 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, as amended, issued a Statement of Reasons (SOR) to the Applicant. The SOR detailed reasons why DOHA could not make the preliminary affirmative finding required under the Directive that it is clearly consistent with the national interest to grant or continue a security clearance for the Applicant. The SOR recommended referral to an Administrative Judge to conduct proceedings and determine whether a clearance should be granted, denied or revoked.

On June 20, 2001, Applicant responded to the allegations set forth in the SOR, and elected to have a decision made by a DOHA Administrative Judge based on the written record; i.e., without a hearing. Department Counsel submitted the Government's File of Relevant Material (FORM) to Applicant on August 7, 2001. The FORM includes 7 exhibits, which have been marked and admitted as Government Exhibits (GX) 1 - 7. The Applicant was instructed to submit information in response to the FORM within 30 days of receipt of the FORM. Through counsel, Applicant submitted a timely response to the FORM, dated September 12, 2001. The matter was assigned to me for resolution on February 11, 2002.

FINDINGS OF FACT

Applicant is a 54-year-old security officer for a defense contractor that is seeking a security clearance for Applicant (level not specified in the FORM materials). The SOR contains four allegations (SOR 1.a - 1.d.) of misuse of information technology systems under Guideline M and one allegation (SOR 2.a.) of personal misconduct under Guideline E, which references the four allegations under Guideline M, cited above. After considering the totality of the evidence in the case file, including Applicant's responses to the SOR and the FORM, I make the following FINDINGS OF FACT as to each SOR allegation:

Guideline M (Misuse of Information Technology)

1.a. - Applicant was reprimanded/counseled/spoken to by a work supervisor sometime in March or April 2000, for

misusing his company computer by using it during work hours for other than official business, to wit: accessing adult chat rooms and other web sites during his work shift. For reasons discussed below, I find the Government has not established that Applicant was reprimanded for accessing "pornographic" web sites (See Applicant's Response to SOR and Response to FORM, and memoranda attached thereto).[(1)] Nothing in the FORM establishes that the web sites visited by Applicant contained pornographic or obscene material as those terms are defined under Federal law, regulation, or judicial precedent. In this regard, I note that Applicant's conduct is not alleged under Guideline D (Sexual Behavior) or Guideline J (Criminal Conduct). In any case, it is not the pornographic or nonpornographic nature of the web sites accessed by Applicant that is the focus of SOR 1.a., but that Applicant was spoken to by his superior because of the cited computer use;

1.b. In December 1999, Applicant was "verbally counseled" by another supervisor, Mr. W, for misusing company computers during working hours;

1.c. From December 1997 to at least June 13, 2000, Applicant visited "adult"and other web sites during working hours at least twice a week. Many of the adult sites involved role playing in bondage situations;

1.d. Applicant continued his personal use of company computers during working hours after being spoken to/counseled as cited in 1.a and 1.b., above. However, he ended such use prior to issuance of specific written company policy on August 29, 2000.

Guideline E (Personal Conduct)

2.a. Applicant's computer-related conduct at work included that cited above in SOR 1.a - 1.d.

POLICIES

Security clearance decisions are not made in a vacuum. DoD Directive 5220.6, as amended,

at Enclosure 2, sets forth policy factors that must be given "binding consideration" in making security clearance determinations. The factors must be followed in every case, according to the pertinent criterion or criteria. However, the factors are neither automatically determinative of the decision in any specific case, nor can they supersede the exercise of an Administrative Judge's common sense and knowledge of relevant law and regulations. Because each security clearance case presents its own facts and circumstances, it cannot be assumed that these factors exhaust the realm of human experience or apply equally in every case. Considering the evidence as a whole, and based on the Findings of Fact set forth above, I find the following specific adjudicative guidelines to be most pertinent to this case:

GUIDELINE M (Misuse of Information Technology)

The Concern: Noncompliance with rules, regulations, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual's trustworthiness, willingness, and ability to protect classified systems, networks and information. Information Technology (IT) Systems include all related equipment used for the communication, transmission, processing, manipulation, and storage of classified or sensitive information.

Conditions that could raise a security concern and may be disqualifying include:

None that are applicable under the facts and circumstances of this matter.[(2)]

(*See,* discussion below).

Conditions that could mitigate security concerns include:

None that are necessary or applicable under the facts and circumstances of this matter.

GUIDELINE E (Personal Conduct)

The Concern: Conduct involving questionable judgment, untrustworthiness, lack of candor, dishonesty, or unwillingness to comply with rules and regulations could indicate that the person may not properly safeguard classified information.

Condition that could raise a security concern and may be disqualifying include:

1. Reliable, unfavorable information provided by associates, employers, coworkers, neighbors, and other acquaintances.

Condition that could mitigate security concerns include:

1. The information was unsubstantiated or not pertinent to a determination of judgment, trustworthiness, or reliability,

The eligibility criteria established by Executive Order 10865 and DoD Directive 5220.6 identify personal characteristics and conduct that are reasonably related to the ultimate question of whether it is "clearly consistent with the national interest" for an individual to hold a security clearance. In reaching the fair and impartial overall common sense determination based on the "whole person" concept required by the Directive, the Administrative Judge is not permitted to speculate, but can only draw those inferences and conclusions that have a reasonable and logical basis in the evidence of record. In addition, as the trier of fact, the Administrative Judge must make critical judgments as to the credibility of witnesses.

In the defense industry, the security of classified information is entrusted to civilian workers who must be counted on to safeguard classified information and material twenty-four hours a day. The Government is therefore appropriately concerned where available information indicates that an applicant for a security clearance, in his or her private life or connected to work, may be involved in conduct that demonstrates poor judgment, untrustworthiness, or unreliability. These concerns include consideration of the potential, as well as the actual, risk that an applicant may deliberately or inadvertently fail to properly safeguard classified information.

An applicant's admission of the information in specific allegations relieves the Government of having to prove those allegations. If specific allegations and/or information are denied or otherwise controverted by the Applicant, the Government has the initial burden of proving those controverted facts alleged in the Statement of Reasons. If the Government meets its burden (either by the Applicant's admissions or by other evidence) and establishes conduct that creates security concerns under the Directive, the burden of persuasion then shifts to the Applicant to present evidence in refutation, extenuation or mitigation sufficient to demonstrate that, despite the existence of conduct that falls within specific criteria in the Directive, it is nevertheless consistent with the interests of national security to grant or continue a security clearance for the Applicant.

A person seeking access to classified information enters into a fiduciary relationship with the Government based upon trust and confidence. As required by DoD Directive 5220.6, as amended, at E2.2.2., "any doubt as to whether access to classified information is clearly consistent with the interests of national security will be resolved in favor of the nation's security."

CONCLUSIONS

The bases for the SOR allegations are substantially statements made by Applicant. In his June 13, 2000 sworn statement to a Defense Security Service (DSS) agent (GX 6), Applicant states:

* I have visited pornographic Internet sites approximately twice weekly since being hired here at [Company A] in Dec[ember]1997. I have used [Company A] computers during duty hours to visit these sites.

* Specifically, these sites were "chat rooms" where I have role played in sexual bondage situations, as well as played trivial games and had general chats. My role-playing has [involved] sexual acts with other people whom I believed are adults. Never knowingly did I have cybersex with minors, nor have I solicited minors for sex. This is my way of meeting interesting people.

* My supervisor verbally reprimanded me in approximately Mar, Apr or May [20]00. Since being counseled by my supervisor, I have continued to visit pornography sites on the Internet using [Company A's] computers during working

hours. I was unaware this violated [Company A] policy.

* I would not allow myself to be blackmailed because of my cybersex.

Although the SOR does not contain any allegations under Guideline D (Sexual Behavior), the term "pornographic" is clearly important to the Government's allegations under Guidelines M and E. For this reason, it has been necessary to determine whether Applicant's use of his company's computers can properly be construed as accessing pornographic web sites and material. I conclude the Government has not shown that some/most/all of the web sites were pornographic/obscene, nor did the Government attempt to do so. Citing company documents attached to the Response to the SOR, Applicant contends Company A policy specifically allowed personal use of the company computers without restriction as to type of use.

After considering all the record evidence, I conclude the weight of the documentation supplied by Applicant shows that while his company had written policies against misuse of the company computers, those policies did not impose either a ban on specific web sites or a general ban against all personal use until August 29, 2000 (*See,* documents in Applicant's responses to SOR). Other than Applicant's use of the term "pornographic" in his sworn statement to a Defense Security Service agent, the term appears only in two DSS Reports of Investigation (ROI) (GX 3 and 4), in which the agent reports what he was told by other persons. Whether the term is a direct quote or a paraphrase by the DSS agent is not clear. I am concerned about the use of the ROIs as exhibits because of the language of Directive 5220.6 paragraph E3.1.20, which states:

Official records of evidence compiled or created in the regular course of business, *other than DoD personnel background reports of investigation (ROI)*, may be received and considered by the Administrative Judge without authenticating witnesses, provided that such information has been furnished by an investigative agency pursuant to its responsibilities in connection with assisting the Secretary of Defense, or the Department or agency head concerned, to safeguard classified information within industry under EO 10865. (Emphasis added).

In the present case, however, since Applicant's Counsel did not object to the inclusion of the two ROIs in the FORM, I find them to be admissible as evidence. At the same time, the pertinent language in the two ROIs, which appears to support SOR allegations 1.a and 1.b., is ambiguous as to whether the pertinent language is a direct quote of what Applicant said to the DSS agent or a paraphrase by the DSS agent of the actual language. Unlike a sworn statement, the Applicant has not signed off on the language used. The fact that the ROIs are admissible does not end the matter. I must still decide the weight to be given the information contained in the ROIs. In the context of the entire record, I find them not to be entitled to controlling weight.

In his response to SOR 1.a., Applicant denies the allegations made therein. While admitting he visited "chat rooms," and using the term "pornographic," he denies noncompliance with his company's rules, procedures, guidelines, or regulations. As I read the four specific disqualifying conditions under Guideline M, the only one that appears pertinent under the totality of the record evidence is E2.A13.1.2.3., since he did use a company computer for personal reasons, i.e., not business-related. However, that Disqualifying Condition requires that the use in question be "specifically prohibited by rules, procedures, guidelines, or regulations." Nothing in the documentation provided by Department Counsel establishes a specific policy, written or oral, prohibiting the personal use alleged against Applicant.

In Applicant's Monthly Performance Review Form signed by his supervisor on January 13, 2000 (Applicant's Response to SOR, Attachment 2), Applicant received generally "Excellent" ratings (eight out of ten), a highly positive evaluation of his "Strong Points," and the following language under "Supervisor suggestion(s) for performance enhancement":

It has been made known to me that [Applicant] may be spending too much time on the internet and not paying enough attention to the monitors on the console. We all, at times, log onto the net, but it is essential that the [alarm console officer, such as Applicant] pay close attention to console activities.

The supervisor referenced in SOR 1.a "counseled discretion" as to Applicant's visits to adult chat rooms "two or three times a week during work hours" in the Spring of 2000 (Response to SOR at p. 4). Company policy memoranda (dated August 19, 1998, November 9, 1998, March 31, 1999, and August 9, 2000), are aimed at more than 20 employees and do not mention "pornographic sites." Neither do other memoranda on the same topic, from other company officials

(Attachment 1 - 5 to GX 3, Applicant's Response to the SOR). Applicant stresses that he accessed the web primarily during "slack periods" of the "swing" and "graveyard" shifts, or while on break during those periods and "did not access the Internet during the day shift" (Applicant's Response to SOR).

The most definitive and documented policy statement having to do with restrictions on computer use is dated August 29, 2000 (last page of Attachment 4 to Applicant's Response to SOR). From the strong language, directed at all plant protection staff, including Applicant, the new policy prohibits all non-official business, regardless of whether it is games, downloading of music, or anything else. One of the ROIs (GX 4), on which the SOR is based is dated April 19, 2001, and states that company written policy was published in the August 29, 2000 memorandum cited above.

I conclude from the above that while Applicant may have acted inappropriately in accessing adult web sites beginning in December 1997, he did not violate specific company rules, procedures, guidelines, or regulations unless such conduct continued after August 29, 2000. There is no evidence that he did so. The supervisor referenced in the ROI admitted as GX 4 states that as far as he knew, Applicant had "discontinued his alleged misuse" and the "matter [was] closed." In his Response to the SOR, Applicant sets the date of his last misuse of the company computer as "just prior to [his] promotion to supervisor on July 16, 2000" and "more than six weeks before" issuance of the August 29, 2000 memorandum establishing the policy prohibiting all nonofficial use.

As to SOR 1.b., the same evaluation applies, since the use alleged occurred around December 1999. While SOR 1.c. may be correct as to numbers of Applicant's visits to the Internet, its reference to "pornographic web-sites" is weakened by a lack of evidence that any or all of the web sites were "pornographic" and/or that Applicant's visits violated any specific company policy. SOR 1.d. is based on the premise that Applicant continued to access pornographic web sites after being informed it was against company policy. However, the record shows that no company policy "specifically prohibiting" use such as Applicant's was issued until after he had stopped all personal use of company computers.

The language of Guideline M's Disqualifying Condition (DC) E2.A13.1.2.3. clearly refers only to computer use that is specifically prohibited. While Applicant's computer use for the purposes cited in the record is certainly in poor taste and not what he is paid to do by his employer, the Government's case does not contain evidence that Applicant's use of the computer, as cited in the SOR, was "specifically prohibited by [his company's] rules, procedures, guidelines, or regulations," at the time of the cited use. On the other hand, Applicant provided substantial documentation to the contrary, i.e., that he stopped his personal use before specific company policy was established.

In his response to the SOR, Applicant submitted Attachment 1, in which the company recognizes and explicitly approves "some incidental and insignificant personal use, . . . subject to management's discretion." The only uses specifically cited as violating company policy do not pertain to Applicant's use. Attachment 3 is an August 19, 1998 memorandum to the plant staff (including but not limited to Applicant), which sets aside a particular "Control Room PC" for "official use only," suggesting that other computers may be accessed for personal use, subject to management discretion, as is provided for in Attachment 1. Other memoranda refer to the use of specific PCs for official use only (Attachment 4, November 9, 1998, November 18, 1998), and computers other than that assigned to the individual in question (Attachment 4 (March 31, 1999).

A memorandum of August 29, 2000 (Attachment 4) is the first one in the evidence of record that states a rule prohibiting use for game playing, music downloading, visiting chat rooms, and/or wandering on the Internet for personal reasons. The last two prohibitions clearly apply to what Applicant was doing, even without reference to pornography.

In January 2000, Applicant informed his supervisor that he had visited adult web sites while on duty (Response to FORM, at Paragraph 1, Attachment B at pp. 2-3). The supervisor counseled discretion but did not tell Applicant to stop accessing the web sites in question (*Id*., at Paragraph 1.a.). Likewise, Applicant's line supervisor, in discussing a pending work evaluation, told Applicant that he should not spend excessive time on the Internet (*Id*. at Para. 1.b.). Both of these admonitions occurred some seven months before the August 29, 2000 memorandum (last page of Attachment 4 to Applicant's Response to SOR), in which the first written (and specific) company policy on computer use to access the Internet was issued. Applicant's last use of company computers to access adult sites was in early July 2000, prior to his being promoted to supervisor on July 16, 2000.

Applicant's responses to the SOR and the FORM raise and document many issues not refuted by the Government.

Overall, the record evidence is heavily weighted in favor of Applicant in terms of: (1) demonstrating that Applicant's use of the company computers for personal activities was not unique to him; (2) was in fact known to his supervisors, who spoke with him about it but did not order him to stop; (3) his being promoted to supervisor in the Summer of 2000; (4) that he stopped on his own because he recognized it was incompatible with his new responsibilities; and (5) that he stopped prior to the issuance of specific company policy prohibiting any personal use.

I conclude from the above that SOR allegations 1.a.,1.b, and 1.c. fail as disqualifying factors because all occurred or ended prior to the August 29, 2000 memorandum specifically prohibiting Applicant's type of computer use. SOR 1.d. likewise fails because Applicant did cease the cited computer use before August 29, 2000. SOR 2.a. fails because it is based on the validity of SOR 1.a. - 1.d. I note the passage of almost 20 months since the last questionable computer use. Considering his positive record at the company, his position and evaluations, I conclude the risk of recurrence is minimal. I have considered the totality of the evidence in light of the appropriate legal standards and factors, and have assessed Applicant's credibility based on the written record. I conclude that Applicant is unlikely to return to the conduct that led him to this adjudication.

FORMAL FINDINGS

Formal Findings as required by Section 3, Paragraph 7 of Enclosure 1 of the Directive are hereby rendered as follows:

Guideline M (Misuse of Information Technology) For the Applicant

Subparagraph 1.a. For the Applicant

Subparagraph 1.b. For the Applicant

Subparagraph 1.c. For the Applicant

Subparagraph 1.d. For the Applicant

Guideline E (Personal Conduct) For the Applicant

Subparagraph 2.a. For the Applicant

DECISION

In light of all 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 Applicant.

BARRY M. SAX

ADMINISTRATIVE JUDGE

1. The term pornography has no specific legal significance. The term of choice used in the Federal courts is "Obscenity." The three part test for determining obscenity in general is found in *Miller v. California*, 413 U.S. 15 (1973). A Congressional restriction on *Miller*, defining "child pornography" appears at 18 U.S.C. 2246.

2. Disqualifying Condition (DC) 1 - There is no evidence that Applicant's entry into the IT system was illegal or unauthorized by his company; (DC 2) - There is no evidence showing that he modified, destroyed, manipulated, or denied access to information on an IT system; (DC 3). His s use of hardware, software, or media from his company's IT system was not specifically authorized, but it wasn't "*specifically prohibited by rules, procedures, guidelines or regulations"* (Emphasis added); (DC 4) There is no evidence Applicant introduced any hardware, software, or media into an IT system without authorization, when specifically prohibited by rules, procedures, guidelines, or regulations.