DATE: September 13, 2002

In Re:

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

Applicant for Security Clearance

CR Case No. 01-03107

REMAND DECISION OF ADMINISTRATIVE JUDGE

BARRY M. SAX

APPEARANCES

FOR GOVERNMENT

Melvin A. Howry, Esquire, Department Counsel

FOR APPLICANT

Louis D. Victorino, Esquire

SYNOPSIS

Applicant used company computer to access adult and sex-related web sites, but stopped before company policy prohibited such use. First decision concluded that such use did not constitute a violation of Misuse of Information Technology Guideline. On remand, I conclude that Applicant's conduct did not constitute a violation of the Personal Conduct guidelines. Clearance granted

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. I issued a Decision on February 15, 2002, in which I found it was clearly consistent with the national interest to grant or continue a security clearance for applicant. The Government appealed the decision and, on August 27, 2002, the DOHA Appeal Board issued an Appeal Board Decision and Remand Order. The case file was returned to me on September 5, 2002, with directions to issue a new decision after correcting the errors identified in the Decision and Remand Order, consistent with my obligations under Directive, Additional Procedural Guidance, Items E3.1.35. And E3.1.25.

As I understand the Appeal Board Decision and Remand Order, I erred by failing to articulate a rational basis for my conclusion as to Guideline E. I have now considered and evaluated Applicant's conduct under Guideline E, and reached conclusions as to how Applicant's conduct should be viewed under that Guideline.

In reaching the following Findings of Fact and Conclusions, I have specifically sought to comply with the Board's directions in correcting the errors cited in its Decision and Remand Order. The Board has directed me to make an independent evaluation of the facts of this case under Guideline E and then to render a final decision in this case based on that independent evaluation.

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 (not a factor in this remand) and one allegation (SOR 2.a.) of personal misconduct under Guideline E. Because SOR 2.a. specifically references the four allegations under Guideline M, cited above, the discussion and findings of fact as to SOR 1.a - 1.d. are also relevant and material in determining how the evidence should be viewed under Guideline E

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 SOR 2.a. under Guideline E (Personal Conduct):

Guideline E (Personal Conduct)

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

of the SOR, as discussed below.

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).

Pornography is a generic term, with no precise legal definition. The closest legal term is "obscenity", which, after many years of imprecise guidance, was finally defined by the U.S. Supreme Court in *Miller v. California* (383 U.S. 413 (1973)), laying out a three-part definition of obscenity, none of which have been established in the present case. 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 or DOHA 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 the Guideline M allegations, but that Applicant was spoken to by his superiors because of the cited excessive computer use.

In December 1999, Applicant was "verbally counseled" by a second supervisor, Mr. W, for misusing company computers during working hours. Again, the record does not establish that all or some of the web sites referenced were in fact legally "pornographic."

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.

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 when he was promoted, which was prior to the issuance of specific written company policy on August 29, 2000.

I also find as follows:

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), and 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 addressed to more than 20 employees (including Applicant) 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 stressed 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 nonofficial business, regardless of whether it is games, downloading of music, or anything else, impliedly including adult or sexually-oriented web sites.

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. But, 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. The totality of the record evidence indicates that Appellant stopped the practice prior to August 29,1997.

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, and November 18, 1998), and computers other than that assigned to the individual in question (Attachment 4 (March 31, 1999).

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.

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 guideline to be most pertinent to this case:

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:

E2.A5.1.2.1. - Reliable, unfavorable information provided by associates, employers, coworkers, neighbors, and other acquaintances.

Condition that could mitigate security concerns include:

E2.A51.2.1. - 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, including specifically 2.a. are substantially statements made by Applicant. In his June 13, 2000 sworn statement to a Defense Security Service (DSS) agent (GX 6), Applicant admitted the nature of his computer use. states:

The Appeal Board has held that "misuse of a computer can be disqualifying under Guideline E even if there was no clear and precise policy against a particular type of computer misuse (ISCR Case No. 98-0265 (March17, 1999) at page 7, cited by Department Counsel in FORM). Unlike the previous case, the present matter does not involve issues alleged under Guideline D (Sexual Behavior). However, the term "pornographic" is clearly important to the Government's allegation under Guideline E, since it is mentioned directly or indirectly in all four SOR allegations on which the single Guideline E allegation is based.

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. Considering all of the record information, I conclude the evidence of record does not show 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.

Applicant uses the term "pornographic" in his sworn statement to a Defense Security Service agent (GX 6). As a general rule, an admission relieves the Government of having to independently prove the allegation. In the present case, however, Applicant's admission that he accessed the Internet as cited in the SOR does not necessarily mean that he is correct that what he was viewing was "pornographic" by relevant legal standards.

Overall, the record evidence demonstrates that Applicant's use of the company computers for personal activities: (1) 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) did not prevent him from being promoted to supervisor in the Summer of 2000; (4) was stopped on his own volition because he recognized it was incompatible with his new responsibilities; and (5) was stopped prior to the issuance of specific company policy prohibiting any personal use.

The core issue on remand is how the above information and facts, as discussed above, should be viewed under Guideline E. Even though this case does not involve any allegations made under Guideline D (Sexual Behavior), such behavior is clearly relevant to any reasoned decision. The facts of record in the present case do not come anywhere near the *egregious* end of the spectrum of adult or sexual-related activities, such as child pornography or violence against women. The real issue is whether Applicants admitted misuse of the company computer raises a doubt about his ability and/or willingness to protect the nation's secrets. I conclude that however tasteless and even questionable Applicant's conduct may have been to others, it does not rise to the level of making him a risk to national security.

Viewing what he did under Guideline E, I conclude that DC 2 and DC 3 are inapplicable since there is no evidence of any falsifications or omissions and DC 6 is inapplicable because there is no evidence of his association with persons involved in criminal activities.

DC 4 might have been applicable in that Applicant's conduct might have increased his vulnerability except that is now too far in the past and too widely known to constitute a risk. DC 5 is not applicable since there is no pattern of dishonesty or rule violations alleged or suggested by the record, since the company rules and policies that could or would have covered Applicant's conduct were not issued until after the conduct stopped

DC 1 may be applicable in that there was "reliable, unfavorable information provided by associates, employers, coworkers, neighbors, and other acquaintances." The information obtained from others at his company certainly qualifies as "unfavorable" but, as discussed above, it does not rise to the level of making him a risk to fail to protect classified information. Clearly, Applicant's use of the company computers did not violate specific written policies, nor did it result in any punitive action by the company.

The people who know him best in the context of this matter are those at his company. From what is in the record, as discussed above, his superiors counseled him but still thought highly enough of him to promote him, even after learning of his computer use. Again, while Applicant was "cautioned" about his excessive use of the computer (FORM at page 5), he was not censured, reprimanded, fined, or otherwise disciplined. In this context, I give considerable weight to his company's favorable action toward Applicant.

The real question is whether Applicant's conduct, as alleged in SOR 1.a. - 1.d., and incorporated by reference into SOR

2.a., constitutes the "questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations [that] could indicate [he] may not properly safeguard classified information" (Directive, Guideline E).

I conclude that a case has not been made under Guideline E (SOR 2.a.) because cause the underlying facts in this case do not establish the questionable judgment, unreliability and/or untrustworthiness that would make him a risk to the proper safeguarding of classified information.

Of all the Mitigating Conditions, only MC 1 is applicable, in the sense that the negative information was legally unsubstantiated, or at least not shown by the Government to be substantiated. If DC 4 is applicable, then MC 5 is also applicable and more persuasive, since his conduct is now more widely known and consequently less likely to result in any pressure being placed on him.

Overall, considering his positive record at the company, his position and evaluations, I conclude the risk of recurrence is minimal. In complying with the directions of the Appeal Board, 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 the evidence favorable to Applicant significantly outweighs the unfavorable evidence (ISCR Case No. 98-0265 (March 19, 1999) at page 3).

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

Subparagraphs 1.a - 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

DATE: September 13, 2002

In Re:

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

Applicant for Security Clearance

)

ISCR Case No. 01-03107

REMAND DECISION OF ADMINISTRATIVE JUDGE

BARRY M. SAX

APPEARANCES

FOR GOVERNMENT

Melvin A. Howry, Esquire, Department Counsel

FOR APPLICANT

Louis D. Victorino, Esquire

SYNOPSIS

Applicant used company computer to access adult and sex-related web sites, but stopped before company policy prohibited such use. First decision concluded that such use did not constitute a violation of Misuse of Information Technology Guideline. On remand, I conclude that Applicant's conduct did not constitute a violation of the Personal Conduct guidelines. Clearance granted

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. I issued a Decision on February 15, 2002, in which I found it was clearly consistent with the national interest to grant or continue a security clearance for applicant. The Government appealed the decision and, on August 27, 2002, the DOHA Appeal Board issued an Appeal Board Decision and Remand Order. The case file was returned to me on September 5, 2002, with directions to issue a new decision after correcting the errors identified in the Decision and Remand Order, consistent with my obligations under Directive, Additional Procedural Guidance, Items E3.1.35. And E3.1.25.

As I understand the Appeal Board Decision and Remand Order, I erred by failing to articulate a rational basis for my conclusion as to Guideline E. I have now considered and evaluated Applicant's conduct under Guideline E, and reached conclusions as to how Applicant's conduct should be viewed under that Guideline.

In reaching the following Findings of Fact and Conclusions, I have specifically sought to comply with the Board's directions in correcting the errors cited in its Decision and Remand Order. The Board has directed me to make an independent evaluation of the facts of this case under Guideline E and then to render a final decision in this case based on that independent evaluation.

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 (not a factor in this remand) and one allegation (SOR 2.a.) of personal misconduct under Guideline E. Because SOR 2.a. specifically references the four allegations under Guideline M, cited above, the discussion and findings of fact as to SOR 1.a - 1.d. are also relevant and material in determining how the evidence should be viewed under Guideline E

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 SOR 2.a. under Guideline E (Personal Conduct):

Guideline E (Personal Conduct)

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

of the SOR, as discussed below.

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).

Pornography is a generic term, with no precise legal definition. The closest legal term is "obscenity", which, after many years of imprecise guidance, was finally defined by the U.S. Supreme Court in *Miller v. California* (383 U.S. 413 (1973)), laying out a three-part definition of obscenity, none of which have been established in the present case. 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 or DOHA 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 the Guideline M allegations, but that Applicant was spoken to by his superiors because of the cited excessive computer use.

In December 1999, Applicant was "verbally counseled" by a second supervisor, Mr. W, for misusing company computers during working hours. Again, the record does not establish that all or some of the web sites referenced were in fact legally "pornographic."

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.

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 when he was promoted, which was prior to the issuance of specific written company policy on August 29, 2000.

I also find as follows:

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), and 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 addressed to more than 20 employees

(including Applicant) 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 stressed 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 nonofficial business, regardless of whether it is games, downloading of music, or anything else, impliedly including adult or sexually-oriented web sites.

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. But, 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. The totality of the record evidence indicates that Appellant stopped the practice prior to August 29,1997.

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, and November 18, 1998), and computers other than that assigned to the individual in question (Attachment 4 (March 31, 1999).

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.

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 guideline to be most pertinent to this case:

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:

E2.A5.1.2.1. - Reliable, unfavorable information provided by associates, employers, coworkers, neighbors, and other acquaintances.

Condition that could mitigate security concerns include:

E2.A51.2.1. - 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, including specifically 2.a. are substantially statements made by Applicant. In his June 13, 2000 sworn statement to a Defense Security Service (DSS) agent (GX 6), Applicant admitted the nature of his computer use. states:

The Appeal Board has held that "misuse of a computer can be disqualifying under Guideline E even if there was no clear and precise policy against a particular type of computer misuse (ISCR Case No. 98-0265 (March17, 1999) at page 7, cited by Department Counsel in FORM). Unlike the previous case, the present matter does not involve issues alleged under Guideline D (Sexual Behavior). However, the term "pornographic" is clearly important to the Government's allegation under Guideline E, since it is mentioned directly or indirectly in all four SOR allegations on which the single Guideline E allegation is based.

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. Considering all of the record information, I conclude the evidence of record does not show 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.

Applicant uses the term "pornographic" in his sworn statement to a Defense Security Service agent (GX 6). As a general rule, an admission relieves the Government of having to independently prove the allegation. In the present case, however, Applicant's admission that he accessed the Internet as cited in the SOR does not necessarily mean that he is correct that what he was viewing was "pornographic" by relevant legal standards.

Overall, the record evidence demonstrates that Applicant's use of the company computers for personal activities: (1) 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) did not prevent him from being promoted to supervisor in the Summer of 2000; (4) was stopped on his own volition because he recognized it was incompatible with his new responsibilities; and (5) was stopped prior to the issuance of specific company policy prohibiting any personal use.

The core issue on remand is how the above information and facts, as discussed above, should be viewed under Guideline E. Even though this case does not involve any allegations made under Guideline D (Sexual Behavior), such behavior is clearly relevant to any reasoned decision. The facts of record in the present case do not come anywhere near the *egregious* end of the spectrum of adult or sexual-related activities, such as child pornography or violence against women. The real issue is whether Applicants admitted misuse of the company computer raises a doubt about his ability and/or willingness to protect the nation's secrets. I conclude that however tasteless and even questionable Applicant's conduct may have been to others, it does not rise to the level of making him a risk to national security.

Viewing what he did under Guideline E, I conclude that DC 2 and DC 3 are inapplicable since there is no evidence of any falsifications or omissions and DC 6 is inapplicable because there is no evidence of his association with persons involved in criminal activities.

DC 4 might have been applicable in that Applicant's conduct might have increased his vulnerability except that is now too far in the past and too widely known to constitute a risk. DC 5 is not applicable since there is no pattern of dishonesty or rule violations alleged or suggested by the record, since the company rules and policies that could or would have covered Applicant's conduct were not issued until after the conduct stopped

DC 1 may be applicable in that there was "reliable, unfavorable information provided by associates, employers, coworkers, neighbors, and other acquaintances." The information obtained from others at his company certainly qualifies as "unfavorable" but, as discussed above, it does not rise to the level of making him a risk to fail to protect classified information. Clearly, Applicant's use of the company computers did not violate specific written policies, nor did it result in any punitive action by the company.

The people who know him best in the context of this matter are those at his company. From what is in the record, as discussed above, his superiors counseled him but still thought highly enough of him to promote him, even after learning of his computer use. Again, while Applicant was "cautioned" about his excessive use of the computer (FORM at page 5), he was not censured, reprimanded, fined, or otherwise disciplined. In this context, I give considerable weight to his company's favorable action toward Applicant.

The real question is whether Applicant's conduct, as alleged in SOR 1.a. - 1.d., and incorporated by reference into SOR 2.a., constitutes the "questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations [that] could indicate [he] may not properly safeguard classified information" (Directive, Guideline E).

I conclude that a case has not been made under Guideline E (SOR 2.a.) because cause the underlying facts in this case do not establish the questionable judgment, unreliability and/or untrustworthiness that would make him a risk to the proper safeguarding of classified information.

Of all the Mitigating Conditions, only MC 1 is applicable, in the sense that the negative information was legally unsubstantiated, or at least not shown by the Government to be substantiated. If DC 4 is applicable, then MC 5 is also applicable and more persuasive, since his conduct is now more widely known and consequently less likely to result in any pressure being placed on him.

Overall, considering his positive record at the company, his position and evaluations, I conclude the risk of recurrence is minimal. In complying with the directions of the Appeal Board, 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 the evidence favorable to Applicant significantly outweighs the unfavorable evidence (ISCR Case No. 98-0265 (March 19, 1999) at page 3).

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

Subparagraphs 1.a - 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