DATE: September 13, 2002

In Re:

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

Applicant for Security Clearance

ISCR Case No. 01-24084

DECISION OF ADMINISTRATIVE JUDGE

DARLENE LOKEY ANDERSON

APPEARANCES

FOR GOVERNMENT

Martin H. Mogul, Department Counsel

FOR APPLICANT

Pro Se

SYNOPSIS

The Applicant's improper use of his company computer to access pornographic sites on the Internet, in violation of company policy has been mitigated. The Applicant's deliberate falsifications in a sworn statement before an agent from the Defense Security Service concerning his improper use of the company computer and inappropriate comments made to a female coworker, have not been mitigated by sufficient evidence of rehabilitation. Clearance is denied.

STATEMENT OF THE CASE

On May 7, 2002, the Defense Office of Hearings and Appeals (DOHA), pursuant to Executive Order 10865 (as amended), and Department of Defense Directive 5220.6 (Directive), dated January 2, 1992, issued a Statement of Reasons (SOR) to the Applicant, which detailed the 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 the Applicant and recommended referral to an Administrative Judge to determine whether a clearance should be denied or revoked.

The Applicant responded to the SOR in writing on May 31, 2002, in which he elected to have the case determined on a written record in lieu of a hearing. Department Counsel submitted the Government's File of Relevant Material (FORM) to the Applicant on July 11, 2002. The Applicant was instructed to submit information in rebuttal, extenuation or mitigation within 30 days of receipt. Applicant received the FORM on July 23, 2002, and he submitted no response. The case was assigned to the undersigned for resolution on August 28, 2002.

FINDINGS OF FACT

The following Findings of Fact are based on Applicant's Answer to the SOR, and the documents. The Applicant is 58 years of age, and is employed by a defense contractor. He seeks a security clearance in connection with his employment in the defense industry.

Paragraph 1 (Guideline E - Personal Conduct). The Government alleges that the Applicant is ineligible for clearance because he has engaged in conduct involving questionable judgment, untrustworthiness, unreliability, or unwillingness to comply with rules and regulations.

Paragraph 2 (Guideline - Misuse of Information Technology Systems). The Government alleges that the Applicant's noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about his trustworthiness, willingness, and ability to properly protect classified systems, networks, and information.

From 1995 through 1997, the Applicant while employed with a previous employer as a Safety Engineer, downloaded pornographic sites against company policy. At the time, the Applicant was learning about web searches for information and data as part of his safety function. During searches for valid data, an occasional pornography site would be discovered. The Applicant eventually found himself competing with several of the other contractors to see who could out do one another by discovering the raunchiest site and the most sites obtainable in a single search. They began to encourage each other. This game became a problem for the female coworkers who worked within the area. (*See*, Government Exhibit 3). The Applicant and the other contractors would also play tricks on each other. On one occasion, the Applicant was going to show a female coworker something on his computer, but as soon as he touched the mouse a centerfold screen saver appeared. (*See*, Government Exhibit 3). The Applicant stated that he did not consider himself breaking any of the rules because he did not save any of the pictures. Following this incident, the Applicant was verbally reprimanded by management and told that pornographic materials were not allowed on the computers. There is no evidence in the record as to whether the Applicant received any other discipline from his employer for this misconduct.

During this same period, the Applicant also e-mailed off-color and ethnic jokes to his fellow coworkers, which included females. The Applicant states that he never meant them to be offensive or carry a negative message. Until he received some sensitivity training, he did not understand the problem with these jokes. He now attempts to ensure that all e-mail is strictly business related.

On another occasion, the Applicant made inappropriate comments to a female employee, including asking her to have an affair with him. The Applicant states that he did this in an effort to bolster her spirits. The Applicant explained that she was not a very attractive person, but on that particular day she had made a special effort to look nice and carry herself in a very happy way. He thought it would help her by making statements that showed that she is the type of woman that men would like to be with.

Most recently, while employed with his present employer, the Applicant installed his personal copy of a software program on his work computer without permission to do so. When it was brought to his attention, he did coordinate with computer support and discovered that the software was going to be installed on all work computers at some point. The Applicant was ultimately allowed to leave his personal software on his computer until the corporate version was installed.

Paragraph 3 (Guideline J - Criminal Conduct). The Government alleges that the Applicant is ineligible for clearance because he violated Federal law, Title 18, United States Code, Section 1001.

In a signed sworn statement dated October 19, 2000, before an agent from the Defense Security Service, the Applicant stated that he had not viewed or downloaded pornographic material on his work computer while working for his employer. (*See*, Government Exhibit 5).

The Applicant also stated that he did not ask a female worker to have a sexual affair with him and he did not make comments to her about not "getting enough" at home. (*See*, Government Exhibit 5). The Applicant stated that when he was interviewed by the first agent, he could not understand her, and could not recall the incident that she was asking him about. (*See*, Government Exhibit 3).

The Applicant further explained that because the agent was a black female, he felt somewhat constrained by the circumstances and was not able to convey his agreement with the allegations. Additionally, the Applicant states that he felt embarrassed to discuss the details of his pornographic downloading/gamesmanship with his male coworkers. He

also states that he was recovering from an extremely bad period in his life where he had been honest with his statements and was forced to find another job that ultimately became a long-term lay off. (*See*, Government Exhibit 3).

I have been provided no reasonable excuse for the Applicant's failure to reveal the truth about his past personal conduct in his sworn statement dated October 19, 2000. Consequently, the evidence proves that the Applicant has not been completely honest with the Government regarding this information. I find that the Applicant deliberately failed to reveal this information to the Government.

POLICIES

Security clearance decisions are not made in a vacuum. Accordingly, the Department of Defense, in Enclosure 2 of the 1992 Directive sets forth policy factors and conditions that could raise or mitigate a security concern; which must be given binding consideration in making security clearance determinations. These factors should be followed in every case according to the pertinent criterion. However, the conditions are neither automatically determinative of the decision in any case, nor can they supersede the Administrative Judge's reliance on her own common sense. Because each security clearance case presents its own unique facts and circumstances, it cannot be assumed that these factors exhaust the realm of human experience, or apply equally in every case. Based on the Findings of Fact set forth above, the factors most applicable to the evaluation of this case are:

Personal Conduct

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.

Conditions that could raise a security concern:

3. Deliberately providing false or misleading information concerning relevant and material matters to an investigator, security official, competent medical authority, or other official representative in connection with a personnel security or trustworthiness determination.

5. A pattern of dishonesty or rule violations, including violation of any written or recorded agreement made between the individual and the agency;

Condition that could mitigate security concerns:

None.

Misuse of Information Technology Systems

Noncompliance with rules, procedures, guidelines 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. Information Technology 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:

1. Illegal or unauthorized entry into any information technology system;

3. Introduction of hardware, software or media into any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations.

Condition that could mitigate security concerns:

1. The misuse was not recent.

Guideline J (Criminal Conduct)

Conditions that could raise a security concern:

1. any criminal conduct regardless of whether the person was formally charged;

2. a single serious crime or multiple lesser offenses.

Conditions that could mitigate security concerns:

None.

In addition, as set forth in Enclosure 2 of the Directive at page 2-1, "In evaluating the relevance of an individual's conduct, the Administrative Judge should consider the following general factors:

a. The nature and seriousness of the conduct and surrounding circumstances

b. The circumstances surrounding the conduct, to include knowledgeable participation

c. The frequency and recency of the conduct

d. The individual's age and maturity at the time of the conduct

e. The voluntariness of participation

f. The presence or absence of rehabilitation and other pertinent behavior changes

g. The motivation for the conduct

h. The potential for pressure, coercion, exploitation or duress

i. The likelihood of continuation or recurrence."

The eligibility criteria established in the DoD Directive identify personal characteristics and conduct which are reasonably related to the ultimate question, posed in Section 2 of Executive Order 10865, of whether it is "clearly consistent with the national interest" to grant an Applicant's request for access to classified information.

The DoD Directive states, "The adjudicative process is an examination of a sufficient period of a person's life to make an affirmative determination that the person is an acceptable security risk. Eligibility for access to classified information is predicted upon the individual meeting these personnel security guidelines. The adjudicative process is the careful weighing of a number of

variables known as the whole person concept. All available, reliable information about the person, past and present, favorable and unfavorable should be considered in reaching a determination." The Administrative Judge can draw only those inferences or conclusions that have reasonable and logical basis in the evidence of record. The Judge cannot draw inferences or conclusions based on evidence which is speculative or conjectural in nature. Finally, as emphasized by President Eisenhower in Executive Order 10865, "Any determination under this order . . . shall be a determination in terms of the national interest and shall in no sense be a determination as to the loyalty of the Applicant concerned."

The Government must make out a case under Guideline E (Personal Conduct) and Guideline M (Misuse of Information Technology Systems), and Guideline J (Criminal Conduct) which establishes doubt about a person's judgment, reliability and trustworthiness. While a rational connection, or nexus, must be shown between Applicant's adverse conduct and his ability to effectively safeguard classified information, with respect to sufficiency of proof of a rational connection, objective or direct evidence is not required.

Then, the Applicant must remove that doubt with substantial evidence in refutation, explanation, mitigation or extenuation, which demonstrates that the past adverse conduct, is unlikely to be repeated, and that the Applicant

presently qualifies for a security clearance.

An individual who demonstrates a disregard for security policies and procedure, or who engages in a pattern of rule violations, may be prone to provide information or make decisions that are harmful to the interests of the United States. The Government must be able to place a high degree of confidence in a security clearance holder to abide by all security rules and regulations, at all times and in all places.

CONCLUSIONS

Having considered the evidence of record in light of the appropriate legal standards and factors, and having assessed the Applicant's credibility, this Administrative Judge concludes that the Government has established its case as to all allegations in the SOR, and that Applicant's misuse of information technology systems and his personal and criminal conduct has a direct and negative impact on his suitability for access to classified information.

Considering all of the evidence, the Applicant has not introduced persuasive evidence in rebuttal, explanation or mitigation that is sufficient to overcome the Government's case.

The Applicant repeatedly violated his company's policy prohibiting the use of his company computer on company time to access pornographic sites from 1995 until 1997. The Applicant knew at the time that he was violating the company policies, but because he was so wrapped up in his gamesmanship with his coworkers, and was not saving the pornographic pictures, he did not feel as though he was breaking the rules. The record does not contain evidence as to whether the Applicant received any verbal or written warnings from his previous employer for his accessing pornographic sites on his company computer, inappropriate comments to female coworker and his off-colored ethnic jokes. This behavior shows poor judgment, however, it has been five years since he engaged in this improperly conduct. Furthermore, other than a verbal reprimand, there is no evidence as to whether the Applicant was ever disciplined for the conduct.

Most recently, the Applicant loaded his personal software on his company computer without permission, however, there is no evidence in the record as to whether he received any warning or discipline for this action or whether it was specifically prohibited by regulation. Given the extent of time that has passed since his last improper access or misuse of company equipment, I find for the Applicant under Guideline M.

With respect to the Applicant's falsifications in his sworn statement dated October 19, 2000 before an agent from the Defense Security Service, I find his explanations to be weak and not credible. The Applicant knew or should have known that when he provided information to the Government, he must be candid, honest, clear and forthright. The Applicant emphatically denied making inappropriate comments to a female coworker and also denied downloading pornographic sites on his company computer during company time when in fact he did so. Consequently, the evidence proves that the Applicant has not been completely honest with the Government regarding this information. I find that the Applicant deliberately failed to reveal this information to the Government.

The Government relies heavily upon the integrity and honesty of clearance holders. It is a negative factor for security clearance purposes when an Applicant has deliberately provided false information about material aspects of his personal background. The Applicant's false statements are also in violation of Section 1001, Title 18 of the United States Code, a felony. This Applicant has not demonstrated that he is trustworthy, and does not meet the eligibility requirements for access to classified information. Accordingly, I find against the Applicant under Guideline E (Personal Conduct) and Guideline J (Criminal Conduct).

The Applicant has not provided this Administrative Judge with sufficient evidence in mitigation that would negate the negative impact his falsifications have on his security worthiness. At this time, I cannot find that it is clearly consistent with the national interests to grant the Applicant a security clearance.

Considering all the evidence, the Applicant has not rebutted the Government's case regarding his personal conduct and criminal conduct. The Applicant has not met the mitigating conditions of Guidelines E, and J of Section F.3. of the Directive. Accordingly, he has not met his ultimate burden of persuasion under Guidelines E and J.

FORMAL FINDINGS

Formal Findings For or Against the Applicant on the allegations in the SOR, as required by Paragraph 25 of Enclosure 3 of the Directive are:

Paragraph 1: Against the Applicant.

Subparas. 1.a.: For the Applicant

1.b.: For the Applicant

1.c.: For the Applicant

1.d.: Against the Applicant

1.e.: Against the Applicant

1.f.: For the Applicant

Paragraph 2: For the Applicant.

Subparas. 2.a.: For the Applicant

Paragraph 3: Against the Applicant.

Subparas. 3.a.: Against the Applicant

DECISION

In light of the circumstances presented by the record in this case, it is not clearly consistent with the interests of national security to grant or continue a security clearance for the Applicant.

Darlene Lokey Anderson

Administrative Judge