DATE: March 25, 2002

In Re:

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

Applicant for Security Clearance

ISCR Case No. 01-02677

DECISION OF ADMINISTRATIVE JUDGE

PAUL J. MASON

APPEARANCES

FOR GOVERNMENT

Michael H. Leonard, Esq., Department Counsel

FOR APPLICANT

Steven N. White, Esq.

SYNOPSIS

The personal conduct allegations are based on Applicant's dishonest and unacceptable conduct in improperly storing pornographic and obscene material on company computers and storage accounts in late 1990. The improper recording of regular and overtime, and excessive use of the Internet for personal reasons such as searching for sales and purchases of toy trucks or other collectibles between September and November 1998, provides the basis for the personal conduct allegations leading to Applicant's dismissal from employment in January 1999. The absence of significant evidence in rehabilitation, as well as evidence reflecting other behavioral changes, requires an ultimate finding against Applicant under the personal conduct guideline. Clearance is denied.

RULINGS ON PROCEDURE

On December 26, 2001, Applicant submitted proposed corrections to the transcript. Those corrections are hereby **accepted**.

STATEMENT OF CASE

On July 26, 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, amended by Change 3, February 13, 1996, and Change 4, April 20, 1999, 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, and recommended referral to an Administrative Judge to determine whether clearance should be denied or revoked. Applicant submitted his response to the SOR on August 16, 2001. Applicant requested a hearing.

The case was transferred to the undersigned on October 30, 2001. A notice of hearing was issued on November 8, 2001, and the case was heard on November 28, 2001. The Government and Applicant submitted documentary evidence. Testimony was taken from Applicant and three witnesses. The transcript (Tr.) was received on December 10, 2001.

FINDINGS OF FACT

The SOR alleges personal conduct (Guideline E). Applicant admitted 1.a., 1.a.(1), and 1.a.(2), but strenuously argued his conduct (1) was either unofficially condoned by his supervisor or (2) grossly exaggerated. Applicant admitted 1.b. but could not answer 1.b.(1) because he did not know whether his conduct was dishonest. He could neither admit nor deny 1.b.(2) alleging his actions constituted unacceptable conduct. Applicant's responses to 1.b.(1) and 1.b.(2) shall be interpreted as denials. Applicant admitted 1.b.(3) as he was cited for neglect of duty and misuse of company time. Applicant's admissions shall be incorporated in the factual findings below, and will be addressed chronologically.

Applicant is 43 years old and has been employed as a principal engineer with a defense contractor since April 1999. He seeks a secret level clearance.

In March 1985, Applicant was hired as an engineer by another defense contractor. On August 5, 1991 (1.b.), Applicant received a Corrective Action emorandum and suspended for one day without pay on August 7, 1991, for violating company rules in December 1990. Those rule violations were: (1) dishonesty for misuse of company materials and supplies (1.b.(1)); (2) unacceptable conduct for storage of pornographic and obscene materials (1.b.(2)); and, (3) neglect of duty in misusing company time (1.b.(3)).

With regard to 1.b.(1), GE 3 (Stipulation of Fact) contains investigative reports leading to Applicant's suspension in August 1991. The 1990 reports contains statements from six individuals who provided statements about Applicant's misuse of company materials and time. In December 1990, the computer administrator for the high technology center discovered Applicant and another employee had used company computers and system accounts for personal purposes. The computer administrator told Applicant the obscene and pornographic material on company computers would have to be deleted. Applicant removed the material by December 21, 1990. The administrator also told Applicant the material could not be transferred to company tapes, which was also property of the company. A second employee of the company indicated to Applicant the obscene material was inappropriate for company computers. A third employee indicated he had seen photos on Applicant's computer in the summer of 1990. The third employee did not think the photos were necessarily obscene, instead considering them tasteful photographs.

A fourth employee (who was investigated with Applicant for collecting the obscene material), indicated Applicant kept his obscene material on disks. Applicant conceded it was, "...probably poor judgment to keep this material on [Company] equipment." Considering all the circumstances surrounding 1.b.(1), I find Applicant's actions exhibited dishonesty as he knew or should have known he was not allowed to accumulate and store obscene pictures on company equipment.

Subparagraph 1.b.(2) alleges unacceptable conduct for storing pornographic and obscene materials on computers and accounts during regular and overtime hours. Even though one of the company employees did not think the material was pornographic or obscene I am reasonably satisfied the material fits the description supplied by most of the witnesses. On balance, Applicant's storage of pornographic and obscene material during regular and overtime business hours represents unacceptable conduct.

The last allegation under paragraph 1 alleges the conduct in 1990, alleged under 1.b.(1) and 1.b.(2) represented neglect of duty for misusing company time. The report demonstrates in fairly extensive detail how Applicant was misusing company materials and supplies by storing obscene material on his company computer and accounts/discs. It is fair to infer the activity was taking Applicant away from his employment-related duties.

Paragraph 1.a. is based on unauthorized activity by Applicant between September and November 1998.[(1)] Paragraph 1.a. alleges Applicant was involuntarily terminated from his position for company rule violations. The rule violations include (1) the improper recording of 66 hours of regular and overtime between September and November 1998, (2) improper use of company personal computer to access the Internet for personal reasons for approximately 101 business hours during regular and overtime hours. This time was primarily spent examining the buying and selling offers for toy trucks and other collectibles. (Tr. 126-128; 145; GE 3)

The basis for Applicant's dismissal in January 1999 is an anonymous complaint by a coworker filed on July 29, 1998, and leading to a security investigation. Part of the investigation focused on the work arrival and departure times of Applicant between September 1, 1998 and November 20, 1998. The monitoring was established by physical surveillance of an access management system, central monitoring kiosk, and a door log containing entry and exit times that are logged and initialed daily. The charts reflect 66 hours of improper time.

According to GE 3, Applicant provided a signed statement on November 30, 1998, to the company security investigator, indicating over the last several months of 1998, he started to abuse his work time by showing up to work late and leaving early in the day. With regard to weekend overtime, Applicant frequently counted his travel time from home to his duty station and back as part of his work time.[(2)] On one weekend, Applicant left work and played basketball, then returned to his work area where he added overtime, even for the time he was at the basketball game.

Between September 1, 1998 and November 9, 1998 (1.a.(2)), Applicant's computer was audited to determine how many hours he spent examining items on the Internet which were unrelated to work. The time Applicant used on the computer to peruse the Internet was divided into his regular work days and overtime days.[(3)] In his signed statement, Applicant stated he spent a lot of time, about two hours a day, both regular and overtime, on the Internet for personal reasons. Applicant spent a lot of time on the internet because he "burnt out" in the job he was in for the last several months.

At the hearing, Applicant provided extensive testimony about why the 101 hour amount (alleged in 1.a.(2)) is exaggerated. First, Applicant noted there were several individuals who had access to this computer in the high technology lab area.[(4)] (Tr. 132) Second, Applicant denied surfing and/or calling up some of the sites listed among the surveillance results in GE 3. (Tr. 132) Third, Applicant disputed the 101 hour figure based on how a computer operates to secure information out of cyberspace. (Tr. 124) Having weighed and balanced Applicant's testimony with his signed statement of November 30, 1998, together with Applicant's interest in the outcome of this proceeding, I find his signed statement (GE 3)is more credible than his testimony.[(5)]

Applicant's second level supervisor at Applicant's current employer, Mr. senior engineer, testified he was a part of the selection process which led to Applicant being hired into requirements management in April 1999. As requirement's manager, Applicant is required to obtain statements of tasking, and all other products needed to perform. Then, as requirements manager, he has to set up a data base to track and house all those requirements. As a requirements manager in cooperative engagement capability (CEC), Applicant must ensure there is a sharing of radar sensor platform capability. Mr. senior engineer was unaware of any security or attendance problems by Applicant /since his hire in April 1999. The senior engineer also had no knowledge of the adverse events at Applicant's previous employer. (Tr. 27) Applicant's performance, according to the senior engineer, exceeded requirements for the period February 2000 to February 2001.

Mr. Program manager supervised Applicant in the 1990s at his previous employer. In the early 1990s, Applicant worked for Mr. program manager as a systems engineer. According to Mr. program engineer, besides developing current security procedures for the high technology lab, Applicant was involved with the security department in developing a procedure where classified material could be erased without having to replace the computer hard drive, thereby allowing someone to use the hard drive for a different purpose. (Tr. 51; 72)

In approximately September 1998, Mr. program engineer recalled Applicant working on 5 projects while translating the customer capability requirements into words on paper. (Tr. 52) After the projects were concluded in September 1998, through selection or de-selection by customers, Applicant's workload slowed dramatically, even though Applicant was still expected to supervise the lab. (Tr. 56)

Mr. program engineer was involved in meetings deciding the sanctions for Applicant's improper recording of work time and improper use of the Internet between September and November 1998. Mr. program engineer recalled the decision of dismissal was preceded by meetings with different personnel, including Applicant and the individuals who lodged the complaints. (Tr. 57) Mr. program engineer would have agreed to a lesser punishment short of dismissal for Applicant. (Tr. 60)

Mr. principal engineer met Applicant in 1985 when they were both members of the same engineering group. According

to Mr. principal engineer, Applicant worked in the high technology lab from 1991 to 1994; then, after working in another section for a period, Applicant returned to the high technology lab in the middle 1990s.

Mr. program engineer recalled the slow period in September 1998 just after the warning system proposal was completed and the team was waiting to see what the customer was going to do. (Tr. 78) During the lull period, Applicant sought other assignments but was denied permission to relocate because his management wanted him at the lab.

Mr. program engineer was never asked to take part in the 1998/early 1999 investigation leading to Applicant's dismissal (Tr. 81), although he knew about other people misusing the Internet. (Tr. 82)

In 1995 and 1996, Applicant was commended for his work in mission systems requirements documentation. Also in 1995 and 1996, he received a favorable mid-term performance evaluation. Applicant received two certificates in 1997 for good performance ratings. (AE D, E) In April 1998, Applicant was recognized for his contributions to configuration management. In September 1998 (AE G), Applicant received congratulations for completing a portion of a project three months ahead of schedule.

Since he has been with his current employer, Applicant's only exposure to security matters was a problem he reported to the security department, and learned the problem was actually a mis-classified document. (Tr. 95) Applicant no longer has responsibility for an entire technical area as he was with his previous employer, because the entire facility is controlled. (Tr. 96)

POLICIES

Enclosure 2 of the Directive sets forth policy factors which must be given consideration in making security clearance determinations. These factors must be considered in every case according to the pertinent criterion; however, the factors are in no way automatically determinative of the decision in any case nor can they supersede the Administrative Judge's reliance on his own common sense. Because each security case presents its own unique facts and circumstances, it should not be assumed that the factors exhaust the entire realm of human experience or that the factors apply equally in every case. In addition, the Judge, as the trier of fact, must make critical judgments as to the credibility of witnesses. Factors most pertinent to evaluation of the facts in this case are:

Personal Conduct

Disqualifying Conditions:

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

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

Mitigating Conditions:

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

General Policy Factors (Whole Person Concept)

Every security clearance case must also be evaluated under additional policy factors that make up the whole person concept. Those factors (found at page 2-1 of Enclosure 2 of the Directive) include: (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; and, (8) the likelihood of continuation or recurrence.

Burden of Proof

As set forth in the Directive, every personnel security determination must be a fair and impartial overall commonsense decision based upon all available information, both favorable and unfavorable, and must be arrived at by applying the standard that the granting (or continuance) of a security clearance under this Directive may only be done upon a finding that to do so is clearly consistent with the national interest. In reaching determinations under the Directive, careful consideration must be directed to the actual as well as the potential risk involved that an applicant may fail to properly safeguard classified information in the future. The Administrative Judge can only draw those inferences or conclusions that have a 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.

The Government must establish all the factual allegations under personal conduct (Guideline E), which establishes doubt about a person's judgment, reliability and trustworthiness. While a rational connection, or nexus, must be shown between an applicant's adverse conduct and her ability to effectively safeguard classified information, with respect to the sufficiency of proof of a rational connection, objective or direct evidence is not required.

Then, Applicant must remove that doubt with substantial evidence in refutation, explanation, mitigation or extenuation which demonstrates that the past adverse conduct is unlikely to repeat itself and Applicant presently qualifies for a security clearance.

CONCLUSIONS

The personal conduct guideline involves acts that demonstrate questionable judgment, untrustworthiness, dishonesty, or unwillingness to comply with rules and regulations. There are two disqualifying conditions (DC) which apply to the circumstances of this case. DC 1 raises security concerns when the adverse information is based on reliable, unfavorable information provided by associates, employers, coworkers, neighbors, and other acquaintances. The foundation for paragraph 1.b. is the investigative report describing Applicant's adverse conduct in late 1990, and leading to his one day suspension in August 1991. The report is comprised of interviews conducted by company security of associates and coworkers (DC 1) who observed the obscene or pornographic material. The other coworker party who was disciplined with Applicant, who had been misusing company equipment and storing obscene material, was also interviewed and confirmed Applicant's involvement. Finally, Applicant provided a signed statement explaining how he collected the information and his opinion that the collection and storage probably constituted poor judgment.

DC 5 (a pattern of dishonesty or rules violations, including a violation of any written or recorded agreement made between the individual and the agency. On August 5, 1991, Applicant received a Corrective Action Memorandum advising him of his suspension for one day in August 1991, without pay for violating company rules. Misusing company computers and system accounts for personal purposes during regular and overtime hours, constitutes a dishonest misuse of company materials and supplies. Storing obscene material on company computers and accounts also represents unacceptable conduct. Applicant's dishonesty and unacceptable conduct also represents a neglect of duty by misusing company time.

MC 1 of the personal conduct guideline is the appropriate mitigating condition for Applicant's misconduct since the adverse information is based on information from employers and coworkers. The first portion of MC 1 must be removed from consideration because I conclude the information from Applicant's coworkers (including the coworker (collector) who was storing the material with Applicant) is reliable because of the consistency of the information from most of the coworkers. Although the information from the collector of obscene material should be scrutinized more carefully in light of his interest in the investigation's outcome, as well as his job, the collector's version of how the material was obtained, collected and displayed to other coworkers, conveys strong corroboration to how the obscene material was actually collected and stored on the computer or disc.

The second portion of MC 1 applies when the information is not pertinent to a determination of judgment, trustworthiness, or reliability. Inappropriately storing pornographic material in company computers or in system accounts/discs is dishonest and unacceptable conduct and amounts to an overall neglect of duty for misusing company time.

Assuming the underlying material is found not to be obscene or pornographic, it was still dishonest and unacceptable conduct for Applicant to misuse or convert company time to his own use.

Since there is no mitigating condition under the personal conduct guideline for DC 5, I must assess Applicant's rules violations under the general factors of the whole person concept. Even though the conduct occurred over ten years ago, the conduct was not isolated in nature and has similarities to the adverse conduct committed by Applicant in 1998. Clearly, the strongest common denominator in the 1990 activity and the 1998 activity was the misuse of company time. On balance, Applicant's 1990 conduct still breeds residual security concerns regarding Applicant's judgment and trustworthiness.

Applicant's improper mis-charging of company time and misuse of the Internet in 1998 for personal reasons, also demonstrates poor judgment and an unwillingness to comply with rules and regulations of the personal conduct guideline. DC 1 receives extensive consideration as the adverse conduct in 1998 was first disclosed by an anonymous coworker through personal surveillance, and confirmed after more than two months of security surveillance, which uncovered improper crediting of work time and abuse of the Internet.

Even without followup security surveillance leading to the figures showing Applicant's misuse of company time and use of the Internet for personal reasons, the underlying information provided by the anonymous coworker is found to be intrinsically reliable because of the accuracy of the information. The reliability of the information is increased after examining the security surveillance results reflecting a large amount of improperly recorded regular and overtime hours. Not to be overlooked is the fact Applicant provided a signed statement and a sworn statement (GE 2) admitting the improper conduct.

The same kind of pattern of dishonesty and rule violations in Applicant's 1990 conduct is present in Applicant's 1998 conduct. In each occurrence, Applicant dishonestly used company regular and overtime. While the figures of misuse of work time and personal time applied to the Internet could be lower than calculated by the security officials, I am persuaded the figures tabulated in GE 3 is more credible than Applicant's impeachment information regarding his work time and the Internet abuse.[(6)]

As there is no corresponding mitigating condition under the personal conduct guideline to evaluate Applicant's conduct in 1998, I again turn to the general factors of the whole person concept to evaluate Applicant's conduct in 1998. The improper recording of time and abuse of the Internet was serious and extensive because it took place regularly between September and November 1998, and not only during the week but also on the weekend. An example of Applicant's brazenness in improperly recording time occurred on one occasion when he left work and played in a basketball game, and did not make the appropriate changes to his time card when he returned. The basketball game example, coupled with Applicant's signed statement explaining why he mis-charged his work time, provide convincing evidence Applicant improperly recorded approximately 66 hours of work time in the September through November work period.

Applicant's excessive use of the Internet to examine deals on toy trucks was serious and extensive. In his signed statement, Applicant admitted he spent about two hours a day on the Internet because he stopped caring about the area he was working in. The foregoing statements spell out the defiant motivation for the conduct in 1998 where Applicant did not even care whether his supervisor knew how Applicant was improperly recording his work time.

Applicant's commendations and other certificates of recognition in the middle 1990s, his contributions in resolving security problems, and Applicant's favorable job performance, represents positive evidence of Appellant's expertise. However, the certificates and performance reports do little to enlighten about what, if any behavioral changes Applicant has made after the 1998 conduct. Given Applicant's misconduct in 1990, the misuse of company time and Internet abuse in 1998, totaling more than 160 hours in a two month period, the lack of security incidents and the fact Applicant does not have the same kind of job as he did in 1998, are insufficient reasons to dispel the negative inferences raised by Applicant's misconduct under the guideline. Applicant was 30 years old when he stored the obscene material on computer/disc. Applicant was 39 years old when he misused company time and improperly bartered over the Internet. Accordingly, Applicant's mitigating evidence falls short of establishing his ultimate burden of persuasion under the whole person concept.

FORMAL FINDINGS

Formal Findings required by Paragraph 25 of Enclosure 3 of the Directive are:

Paragraph 1 (Personal Conduct): AGAINST THE APPLICANT.

a. Against the Applicant.

(1).Against the Applicant.

(2). Against the Applicant.

b. Against the Applicant.

(1) Against the Applicant

(2) Against the Applicant.

(3) Against the Applicant.

DECISION

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

Paul J. Mason

Administrative Judge

1. Applicant's admitted practice of mis charging time actually began one or two months earlier before the official period of surveillance began in September 1998. (Tr. 145)

2. Even though Applicant stated he had the informal approval from his supervisor to count his commute time as work time (Tr. 119-120), I find Applicant, as he indicated in his signed statement of November 30, 1998 (GE 3), never asked his supervisor.

3. As indicated on the computation page of GE 3, the figures reflect access to the top three sites is at least two or more times more than to the bottom five sites.

4. Applicant talked about page counts and how it might take 20 hits to bring up a single page; how recalling the single page may trigger 20 more hits, and then searching and recalling the information may quickly multiply the actual number of page hits. (Tr. 124) Applicant also explained how the computer continues to measure time even though the site has been reached but the computer is unattended. (Tr. 125-127)

5. Applicant repudiates most of his November 30, 1998 statement because it was written by the security investigator and not Applicant, (Tr. 149), and the statement contains inflated figures representing mis-charged time and excessive Internet use. (Tr. 138) According, to Applicant, the investigator threatened Applicant with immediate dismissal if he did not sign the statement. (TR. 136) Even though the statement contained all the incorrect information, Applicant signed the statement anyway because he was ready to move on to a job maximizing his capabilities. (Tr. 138) It is difficult to understand why Applicant would even sign a statement he knew contained so much false information.. Considering all the evidence regarding the credibility of the signed statement, Applicant has failed to provide any independent support as to why the November 1998 statement should not be believed.

6. The sworn statement (GE 2) provides limited support to improper crediting of work time and abuse of the Internet.