DATE: July 18, 2003

In Re:

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

Applicant for Security Clearance

ISCR Case No. 02-12329

DECISION OF ADMINISTRATIVE JUDGE

MATTHEW E. MALONE

APPEARANCES

FOR GOVERNMENT

Catherine Engstrom, Esquire, Department Counsel

FOR APPLICANT

Richard Murray, Esquire

SYNOPSIS

Applicant and his wife have been unable to conceive a child of their own. His wife's only pregnancy resulted in miscarriage after seven months. The resulting psychological effects led Applicant to turn to pornography as an escape. In 1994, he misused his work computer to download and store pornography. Unbeknownst to him, a small percentage of the files he acquired in a large batch download included child pornography. Prosecution was declined due to lack of intent to possess child pornography in violation of federal laws. Applicant resigned in lieu of being fired, a fact he intentionally omitted from his EPSQ. However, the concerns raised by his personal conduct, criminal conduct, and misuse of technology are mitigated through the isolation, lack of recency, and by significant rehabilitation. Clearance is granted.

STATEMENT OF THE CASE

On October 25, 2002, the Defense Office of Hearings and Appeals (SOR) issued to Applicant a Statement of Reasons (SOR) alleging facts which raise security concerns under Guideline J (Criminal Conduct), Guideline E (Personal Conduct), and Guideline M (Misuse of Information Technology Systems). The SOR informed Applicant that, based on information available to the Government, DOHA adjudicators could not make a preliminary affirmative finding that it is clearly consistent with the national interest to continue Applicant's security clearance.[(1)]

Applicant submitted an undated response to the SOR (Answer) in December, 2002. On January 14, 2003, DOHA received from Applicant a more specific Answer in which he admitted some allegations and denied others. The case was assigned to me on March 20, 2003. DOHA subsequently issued a Notice of Hearing setting this case to be heard on April 30, 2003. Thereafter, Applicant retained legal counsel, who requested a continuance to allow adequate time to prepare for hearing. There being no objection by the government, I granted Applicant's request and rescheduled the hearing for May 21, 2003. All parties appeared as scheduled and the Government presented four exhibits (GE 1 through 4), which were admitted as evidence without objection. Applicant relied on four exhibits (AE A through D), which were admitted without objection, his own testimony and the testimony of three other witnesses. DOHA received the transcript (Tr) on May 30, 2003.

FINDINGS OF FACT

Applicant admitted the allegations in SOR subparagraphs 1.a, 3.d, and 3.f. Accordingly, those allegations are entered as facts. After a thorough review of the pleadings, transcript, and exhibits, I make the following additional findings of fact:

Applicant is 43-years-old and works as a video teleconferencing engineer for a defense contractor. He was in the Army between 1985 and 1990, where he was trained in video production and video teleconferencing systems. After leaving the Army, he became a civilian DoD employee working at the same command he was last assigned to before his military discharge.(2)

He has been married since 1988. Applicant and his wife have had difficulty conceiving a child of their own, but, in 1992, Applicant's wife became pregnant. Unfortunately, she miscarried after seven months. This event devastated Applicant and his wife, causing Applicant to withdraw from her and to suffer from depression.

Between 1992 and 1994, Applicant became addicted to pornography which he used as an escape from his emotional and marital problems. In 1994, he accessed an internet site from his computer at work and downloaded over 1,000 pornographic images. He also downloaded related software applications designed to encrypt the material he was downloading and to delete identifying information from his e-mails.

At the time Applicant downloaded pornographic materials, the internet had not yet developed to what is now known as the worldwide web. Rather than pointing to a file or link with a mouse cursor and clicking to access the desired file as is done today, Applicant had to type in a command that caused a "zip" or compressed file to be transferred to his computer. The "zip" file contained the pictures in hundreds of smaller files that could be accessed when Applicant executed another command; but until he executed that command, he could not see the contents or know exactly what the files contained.(3)

Applicant's duties required him to occasionally take unclassified files containing scripts for videos he was working on. These files were loaded onto floppy diskettes and carried between his home computer and his work computer. At some point, Applicant inadvertently loaded information related to his home business on a diskette he was also using to transfer his unclassified work files and loaded his business files onto his work computer.(4)

In 1994, investigators from three federal criminal investigative agencies coordinated an investigation into Applicant's alleged misuse of DoD computer systems. A search of Applicant's work computer and his desk yielded pornography and other unauthorized materials, including personal business information and a variety of software programs supporting possible distribution and viewing of pornography, as well as a variety of work-related downloads. Some of the pornographic images were determined to contain depictions of minors engaged in sexual activities, which was a potential violation of at least two federal criminal statutes.(5)

Applicant admitted to investigators he had intentionally downloaded pornography to his DoD computer but denied knowingly obtaining or possessing child pornography. While he received no specific guidance, and there were no procedures in place governing use of the internet at the time, Applicant knew he was violating DoD rules against use of his work computer for personal or unauthorized purposes.

When the investigation was concluded, Applicant was notified that the U.S. Attorney's office was considering initiating criminal prosecution for violation of 18 U.S.C. §2252 (possession of child pornography), 18 U.S.C. §641 (theft of public money), and 18 U.S.C. §1030 (fraud and related activity in connection with computers). However, prosecution was eventually declined. Subsequently, DoD advised Applicant he would be terminated based on the results of the investigation. When offered the option of resigning in lieu of termination, Applicant resigned and pursued other employment in the video production field.

Applicant was hired by his current employer in November 1998. On December 29, 2000, Applicant executed an electronic security clearance application (EPSQ) from which he omitted the fact that he resigned from DoD under unfavorable circumstances.(6) When Applicant executed the EPSQ, he elected an option that allows suppression of Part 2 of the form so that it cannot be viewed or printed by anyone other than DoD investigators.(7) Applicant averred at hearing that he rushed through the form and that any omission was accidental. He brought the discrepancy to the attention of the investigator when he was interviewed by DSS. (8) After the interview, Applicant submitted a written statement which did not address the matter of his answers to the EPSQ and any possible discrepancies therein.(9)

Around 1993, Applicant and his wife resumed their attempts to have a baby, but were unsuccessful. In September 2001, they adopted a son who is now about two years old. By all accounts, Applicant and his wife have recovered from the stress and tribulations caused by the miscarriage and by Applicant's misconduct at work. Applicant's wife nearly left him over the latter incident, however, he has regained her trust and they have repaired whatever damage their marriage suffered.(10)

After leaving his DoD job, Applicant sought counseling through Sex Addicts Anonymous (SA) in 1996. Over the next year, he completed a 12-step program modeled on the Alcoholics Anonymous approach to alcoholism. He was recently assessed by a licensed professional counselor experienced in addictive behavior, who has expressed a high degree of confidence that Applicant will not repeat his earlier conduct.(11)

Applicant and his wife do not allow pornography in their home and Applicant has installed extensive safeguards on their computer to prevent the introduction of unwanted materials such as pornography. Applicant is active in his church and community. He is also well-regarded by his employer as a valued employee and hard worker. Having observed his demeanor, I found Applicant credible and sincere in taking responsibility for his past misconduct.

POLICIES

The Directive sets forth adjudicative guidelines[(12)] to be considered in evaluating an Applicant's suitability for access to classified information. The Administrative Judge must take into account both disqualifying and mitigating conditions under each adjudicative issue applicable to the facts and circumstances of each case. Each decision must also reflect a fair and impartial common sense consideration of the factors listed in Section 6.3 of the Directive. The presence or absence of a disqualifying or mitigating condition is not determinative of a conclusion for or against an Applicant. However, specific applicable guidelines should be followed whenever a case can be measured against them as they represent policy guidance governing the grant or denial of access to classified information. Having considered the record evidence as a whole, specifically, that Applicant has close ties of affection who are foreign citizens, I conclude the relevant adjudicative guidelines to be applied here are Guideline E (Personal Conduct), Guideline J (Criminal Conduct), and Guideline M (Misuse of Information Technology Systems).

BURDEN OF PROOF

A security clearance decision is intended to resolve whether it is clearly consistent with the national interest[(13)] for an Applicant to either receive or continue to have access to classified information. The Government bears the initial burden of proving, by something less than a preponderance of the evidence, controverted facts alleged in the SOR. If the government meets its burden it establishes a *prima facie* case that it is not clearly consistent with the national interest for the Applicant to have access to classified information. The burden then shifts to the Applicant to refute, extenuate or mitigate the Government's case. Because no one has a "right" to a security clearance, the Applicant bears a heavy burden of persuasion.[(14)] A person who has access to classified information enters into a fiduciary relationship with the Government based on trust and confidence. The Government, therefore, has a compelling interest in ensuring each Applicant possesses the requisite judgement, reliability and trustworthiness of one who will protect the national interests as his or her own. The "clearly consistent with the national interest" standard compels resolution of any reasonable doubt about an Applicant's suitability for access in favor of the Government.[(15)]

CONCLUSIONS

Guideline E (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.[(16)] The government has established its case that Applicant's truthfulness is in question because of an answer he gave in his EPSQ. He omitted relevant information from his EPSQ; specifically, he answered "no" when asked to declare if he had ever been fired from a job or left under unfavorable circumstances. Guideline E Disqualifying Condition (DC) 2[(17)] applies because he deliberately omitted this information from his EPSQ. I do not accept his representations that the omission was inadvertent. Applicant disclosed that he had undergone bereavement counseling after his wife's miscarriage, and he elected to suppress Part 2 of the EPSQ ostensibly to protect his own privacy. In light of this fact, Applicant's claim at hearing that he rushed through the application and simply forgot to disclose the other significant event in his life - his forced resignation from DoD in 1996 - does not make sense.

By contrast, Applicant is entitled to some mitigation under Guideline E. He meets two of the three prongs of Mitigating Condition (MC) 2[(18)] in that this is an isolated incident of falsification, and Applicant corrected his answer to EPSQ Question 20 when he was asked to review his the questionnaire by the DSS agent who interviewed him. I accept Applicant's testimony that he drew the agent's attention to the inaccurate answer Applicant had provided because, had there been a real concern by DSS about deliberate falsification, there would have been some mention of it in Applicant's statement. But for the fact the falsification is a recent event, MC 2 would apply. Likewise, MC 3[(19)] fails because Applicant can reasonably be said to have corrected the falsification before being confronted with the facts, he waited until being interviewed 10 months later before providing the correct information. Therefore, and because the other listed MC's are inapposite to the facts of this case, none of the listed MC's can be applied here.

However, bearing in mind the Directive's proviso that the adjudicative guidelines should be applied in conjunction with Directive Section 2.2.1, and not as inflexible rules of law, I conclude Applicant's falsification in this matter is not so security significant as to be disqualifying. I conclude Guideline E for the Applicant.

Guideline M (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.[(20)]

The government has established its case as alleged in SOR paragraph 3. Applicant knowingly used his DoD computer for unauthorized purposes. He downloaded pornography and other unauthorized materials from the internet and stored them on his DoD computer. He admits doing so and admits he knew such conduct was not allowed. Guideline M DC 4[(21)] applies. However, Guideline M MC 1[(22)] and MC 4[(23)] also apply here. The conduct in question has not been repeated since 1996 and there is no information in the record to suggest this was anything but an isolated event. Further, the underlying causes of his addiction to pornography are no longer present, and he has taken significant rehabilitative steps - SA, counseling, a happier home life, and installation of safeguards on his home PC - that support a conclusion that he is unlikely to repeat this conduct in the future. I conclude Guideline M for the Applicant.

Guideline J (Criminal Conduct). A history or pattern of criminal activity creates doubt about a person's judgment, reliability and trustworthiness.[(24)] The government has not established its case under Guideline J as set forth SOR paragraph 1.a.; specifically, that Applicant "knowingly" violated federal laws governing possession of child pornography and falsification of a statement to an agency of the United States government. The evidence regarding subparagraph 1.a does not show Applicant acted with intent when child pornography was found on his computer. There is no doubt that he deliberately downloaded pornography. However, the manner in which it was downloaded - a batch of files within one large zip file - makes it more likely than not the 1% of the pictures that depicted children were included without Applicant's knowledge. This appears to be one of the reasons the Department of Justice declined prosecution in this matter. It has not been alleged that simply downloading pornography is a criminal act. The specific criminality here concerns the acquisition and possession of child pornography, and the federal statute on this matter is quite clear in its requirement of specific intent to do so.

The government has established its case under subparagraph 1.b that Applicant deliberately falsified his EPSQ, a violation of 18 U.S.C. §1001. Guideline J DC 2[(25)] applies. However, Applicant is also entitled to MC 2[(26)] as this is the only such conduct supported by the information in this case. On balance, and in light of all of the evidence which demonstrates that Applicant is not likely to repeat this conduct, I conclude Guideline J for the Applicant.

I have carefully weighed all of the evidence in this case, and I have applied the aforementioned disqualifying and mitigating conditions as listed under each applicable adjudicative guideline. I have also considered the whole person concept as contemplated by the Directive in Section 6.3, and as called for by a fair and commonsense assessment of the record before me as required by Directive Section E2.2.

FORMAL FINDINGS

Formal findings regarding each SOR allegation as required by Directive Section E3.1.25 are as follows:

Paragraph 1, Criminal Conduct (Guideline J): FOR THE APPLICANT

Subparagraph 1.a: For the Applicant

Subparagraph 1.b: For the Applicant

Paragraph 2, Personal Conduct (Guideline E): FOR THE APPLICANT

Subparagraph 2.a: For the Applicant

Paragraph 3, Misuse of Technology (Guideline M): FOR THE APPLICANT

Subparagraph 3.a: For the Applicant

Subparagraph 3.b: For the Applicant

Subparagraph 3.c: For the Applicant

Subparagraph 3.d: For the Applicant

Subparagraph 3.e: For the Applicant

Subparagraph 3.f: For the Applicant

Subparagraph 3.g: 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 the Applicant.

Matthew E. Malone

Administrative Judge

1. Required by Executive Order 10865, as amended, and by DoD Directive 5220.6 (Directive), as amended.

2. Tr., p. 21 - 22; GE 1.

3. Tr., p. 33 - 34.

4. Tr., p. 32.

5. GE 3, AE A.

6. GE 2, Question 20.

7. This accounts for the introduction of two versions of the same form in GE 1 and GE 2. The latter is a print out of the entire form as it was transmitted to the Defense Security Service after Applicant completed it.

8. Tr., p. 29.

9. GE 4, AE B.

10. Tr., p. 72 - 75.

11. AE D.

12. Directive, Enclosure 2.

13. *See Department of the Navy v. Egan*, 484 U.S. 518 (1988).

14. *See Egan,* 484 U.S. at 528, 531.

15. *See Egan;* Directive E2.2.2.

16. Directive, E2.A5.1.1.

17. E2.A5.1.2.2. The deliberate omission, concealment, or falsification of relevant and material facts from any personnel security questionnaire, personal history statement, or similar form used to conduct investigations,

determine employment qualifications, award benefits or status, determine security clearance eligibility or trustworthiness, or award fiduciary responsibilities;

18. E2.A5.1.3.2. The falsification was an isolated incident, was not recent, *and* the individual has subsequently provided correct information voluntarily; (emphasis added).

19. E2.A5.1.3.3. The individual made prompt, good-faith efforts to correct the falsification before being confronted with the facts;

20. Directive, E2.A13.1.1.

21. E2.A13.1.2.4. Introduction of hardware, software or media into any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations;

22. E2.A13.1.3.1. The misuse was not recent or significant;

23. E2.A13.1.3.4. The misuse was an isolated event;

24. Directive, E2.A10.1.1.

25. E2.A10.1.2.2. A single serious crime or multiple lesser offenses.

26. E2.A10.1.3.2. The crime was an isolated incident;