DATE: October 31, 2006

In Re:

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

Applicant for Security Clearance

ISCR Case No. 05-17974

DECISION OF ADMINISTRATIVE JUDGE

CLAUDE R. HEINY

APPEARANCES

FOR GOVERNMENT

Richard A. Stevens, Department Counsel

FOR APPLICANT

David E. Wheeler Esquire

SYNOPSIS

In 2002 or 2003, Applicant created a personal website on his company's computer. When discovered, it was removed, he received a verbal reprimand, and told not to do it again, which he has not done. In 2003 or 2004, Applicant called his former employer's voice mail system and deleted some of his ex-wife's messages and those of the company's president. When told to stop, he did and has not repeated his actions. The record evidence is sufficient to mitigate or extenuate the negative security implications. Clearance is granted.

STATEMENT OF THE CASE

On April 13, 2006, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) to Applicant, stating that DOHA could not make the preliminary affirmative finding[(1)] it is clearly consistent with the national interest to grant or continue a security clearance for Applicant. The SOR set forth reasons why an affirmative finding could not be made that it is clearly consistent with the interests of national security to grant or continue a security clearance for Applicant due to Misuse of Information Technology Systems and Personal Conduct security concerns.

On May 31, 2006, Applicant answered the SOR and requested a hearing. On June 20, 2006, I was assigned the case. On August 18, 2006, a Notice of Hearing was issued for the hearing held on September 13, 2006. On September 21, 2006, DOHA received a copy of the transcript (Tr.). The record was kept open to allow Applicant to submit additional documents, which were received on October 2, 2006. Department Counsel having no objections, the documents were admitted into evidence.

FINDINGS OF FACT

The SOR alleges security concerns for the Misuse of Information Technology Systems and Personal Conduct. Applicant admits to the following: he loaded software on his company computer without approval. He also admitted he was

previously the system manager of the voice mail and telephone system at his former employer. After leaving the company, he used his ex-wife's and former boss's passwords to delete some messages. The admissions are incorporated herein as findings of fact. After a thorough review of the entire record, I make the following additional findings of fact.

Applicant is a 49 year old senior electronics technician who worked for a defense contractor since March 1998, and is seeking to maintain a top-secret security clearance. A principle engineer and the security officer at Applicant's current job believes Applicant is trustworthy, reliable, hard working, and an honest employee. (App Ex A and B) Applicant's most recent performance evaluation lists his overall job performance as exceeding expectations. (App Ex C)

Applicant's company has an acceptable use policy which prohibits playing computer games during work hours, but allows one to communicate with friends and family. Use of the computer is allowed so long as it does not cause problems with the equipment or involve a large amount of data. (Tr. 29) While using a chat program, similar to an instant messaging program, Applicant was given the option to activate a personal home web page. Not knowing the full ramifications of his action, he checked the block to create the page. This was done on this company's computer. Shortly thereafter, he was notified the web page was being removed and not to do it again. He received a verbal reprimand. (Tr. 28) His internet access was removed for a month or two before being restored. The incident had no impact on his pay, promotions, or job evaluations. (Tr. 50) Since the incident, Applicant has not put any programs on his company computer and uses only the software approved and provided by the company.

From 1982 to 1998, Applicant worked at a full service music store that had approximately 60 employees selling music and instruments as well as repairing musical instruments. Applicant started as an electronics technician repairing instruments and, at one time, was in charge of the company's inventory. The president of the company asked him to purchase and set up a new telephone system for the store, which included voice mail. As system manager, Applicant was given his boss's password, that of his now ex-wife, who still works at the company, and that of a subordinate. His ex-wife is the executive assistant and personal secretary for the president of the company. (Tr. 47) After leaving the company in 1998, he was asked at various times to come back to do consulting work for the company on different issues. (Tr. 24)

In 2003 or 2004, five or so years after leaving the company, Applicant used his then wife's password and that of his former boss on six to eight occasions to access the voice mail system and deleted voice mail messages. The president of the company contacted him and asked him to stop his action if he was the one doing it, which he did. (Tr. 43) No criminal action was taken in this matter.

Applicant married in December 1981, separated in December 2003, and divorced in December 2004. At the time of his actions, Applicant was in the midst of a divorce proceeding which was proceeding slowly. It was a period of general frustration in his life. His action of calling the voice mail system was out frustration. At the time, Applicant was on anti-depressants which were not helping him cope with his depression. A change of medication helped greatly with his depression. Following his actions, he felt sorry, embarrassed, and felt bad. Applicant recognizes this was wrong, stupid, unprovoked, and regrets doing it. (Tr. 24, 26) He regrets his actions. (Tr. 57) He would never repeat such conduct.

POLICIES

The Directive sets forth adjudicative guidelines to be considered when evaluating a person's eligibility to hold a security clearance. Disqualifying Conditions (DC) and Mitigating Conditions (MC) are set forth for each applicable guideline. Additionally, each decision must be a fair and impartial commonsense decision based upon the relevant and material facts and circumstances, the whole person concept, and the factors listed in Section 6.3 of the Directive. The adjudicative guidelines are to be applied by administrative judges on a case-by-case basis with an eye toward making determinations that are clearly consistent with the interests of national security. The presence or absence of a particular condition or factor for or against clearance is not determinative of a conclusion for or against an applicant. However, the adjudicative guidelines should be followed whenever a case can be measured against this policy guidance. Considering the evidence as a whole, I conclude the relevant guidelines to be applied here are Guideline M, Misuse of Information Technology Systems, and Guideline E, Personal Conduct.

BURDEN OF PROOF

The sole purpose of a security clearance decision is to decide if it is clearly consistent with the national interest to grant or continue a security clearance for an applicant. Initially, the Government must establish, by substantial evidence, that conditions exist in the personal or professional history of the applicant which disqualify, or may disqualify, an applicant from being eligible for access to classified information. The burden of proof in a security clearance case is something less than a preponderance of evidence, although the government is required to present substantial evidence to meet its burden of proof. Substantial evidence is more than a scintilla, but less than a preponderance of the evidence. All that is required is proof of facts and circumstances which indicate an applicant is at risk for mishandling classified information, or that an applicant does not demonstrate the high degree of judgment, reliability, or trustworthiness required of persons handling classified information. Additionally, the government must prove controverted facts alleged in the SOR. Once the government has met its burden, the burden shifts to an applicant to present evidence to refute, extenuate or mitigate government's case. Additionally, an applicant has the ultimate burden of persuasion to obtain a favorable clearance decision.[(2)]

As noted by the United States Supreme Court in *Department of Navy v. Egan*, 484 U.S. 518, 528 (1988), "no one has a 'right' to a security clearance." 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. The "clearly consistent with the national interest" standard compels resolution of any reasonable doubt about an applicant's suitability for access to classified information in favor of protecting national security. Security clearance determinations should err, if they must, on the side of denials.

CONCLUSIONS

The Government has satisfied its initial burden of proof under Misuse of Information Technology Systems. Applicant created a personal website on his company's computer. This was an unauthorized modification of an informational technology system and introduction of software into an information technology system without authorization. However, there is no showing the introduction of software was specifically prohibited by rules, procedures, guidelines or regulations.

While on the chat program, Applicant did not know the full ramifications of choosing to create a personal web page. It was an intentional action on his part to check to block to activate a home page, but the ramifications were unintentional or inadvertent. Misuse of Information Technology Systems Mitigating Condition (MC) 2 (The conduct was unintentional or inadvertent) applies. As a result of his action, his internet access was denied for two months, but his actions did not result in the loss of money or promotion, but only in a verbal reprimand. Applicant was told not to do it again and never has. This was the single time Applicant ever did any thing of this nature. MC 4 (The misuse was an isolated event) applies. The misuses of information technology systems security concern has been mitigated. I find for Applicant as to SOR 1 and 1.a.

Conduct involving questionable judgment, untrustworthiness, unreliability, or unwillingness to comply with rules and regulations could indicate that the person may not properly safeguard classified information.

Personal conduct is always a security concern because it asks the central question does the person's past conduct justify confidence the person can be trusted to properly safeguard classified information. Applicant put a personal web page on his company computer and called his prior employer's voice mail system and deleted voice messages from his ex-wife's telephone and that of the company's president's telephone.

Applicant acknowledges his actions were stupid and immature. He has thought a great deal about his conduct. Once he was told not to do it again, he stopped. Applicant was undergoing a period of general frustration. I have considered the nature, extent, and seriousness of the conduct. I have also considered Applicant's age and maturity at the time of the conduct; the circumstances surrounding the conduct; the motivation for the conduct (Applicant acknowledges he acted inappropriately); the frequency (six to eight times) and recency of the conduct (2003 or 2004); presence or absence of rehabilitation; and potential for pressure, coercion, exploitation, or duress.

In considering the probability that the circumstance or conduct will continue or recur in the future, I believe Applicant is

sincere when he says he will only use software provided by his current company and will never again call his former employer's voice mail system. I find for Applicant as to Personal Conduct.

FORMAL FINDINGS

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

Paragraph 1 Misuse of Information

Technology Systems: FOR APPLICANT

Subparagraph 1.a.: For Applicant

Paragraph 2 Personal Conduct: FOR APPLICANT

Subparagraph 2.a.: For Applicant

Subparagraph 2.b.: For 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. Clearance is granted.

Claude R. Heiny

Administrative Judge

1. Required by Executive Order 10865, as amended, and Department of Defense Directive 5220.6 (Directive), dated January 2, 1992, as amended.

2. ISCR Case No. 93-1390 (January 27, 1995) at pp. 7-8; Directive, Enclosure 3, Item E3.1.15