DATE: March 8, 2005

In Re:

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

Applicant for Security Clearance

ISCR Case No. 02-31325

DECISION OF ADMINISTRATIVE JUDGE

CLAUDE R. HEINY

APPEARANCES

FOR GOVERNMENT

Jason Perry, Department Counsel

FOR APPLICANT

Pro Se

SYNOPSIS

Applicant accessed sexually explicit internet sites on company computers three times at his previous job. He was verbally reprimanded, then received a ten-day suspension, and finally terminated when the conduct continued. At his current job, he has twice accessed sexually explicit sites in violation of company rules. The record evidence is insufficient to mitigate or extenuate the negative security implications stemming from misuse of information technology systems and personal conduct. Clearance is denied.

STATEMENT OF THE CASE

On January 14, 2004, 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. On February 11, 2004, Applicant answered the SOR and elected to have his case decided on the written record in lieu of a hearing.

On July 7, 2004, the Applicant received a complete copy of the file of relevant material (FORM) dated June 15, 2004, and was given the opportunity to file objections and submit material in extenuation, mitigation, or refutation. On August 6, 2004, the Applicant's response to the FORM was due. No response has been received. On February 1, 2005, I was assigned the case.

FINDINGS OF FACT

The SOR alleges as security significant the misuse of information technology systems and personal conduct. The Applicant admits to the following: in 1998, he received a verbal reprimand for accessing sexually explicit internet sites without authorization on his employer's computer; in 1999, he was suspended for ten days for the same reason; in 2000, he was terminated for the same reason; and, in 2002, he again accessed sexually explicit sites without authorization while working for his current employer. Those admissions are incorporated herein as findings of fact. After a thorough

review of the entire record, I make the following additional findings of fact:

The Applicant is 60 years old and has worked as a security officer for a defense contractor since January 2001, and is seeking to obtain a security clearance.

In 1998, Applicant first accessed a sexually explicit internet site without authorization on his employer's computer. His action was quickly discovered by his employer and within a week he received a very strong talking to by his department manager. His internet access was revoked for a year. In August 1999, shortly after his access was restored, he again viewed sexually explicit sites at work. He received a mandatory, ten-day suspension. His internet access was again revoked for a year. In 2000, shortly after his access was restored, he again accessed a sexually explicit internet site. In September 2000, he was offered immediate early retirement for his misconduct. If he did not accept retirement, his company would initiate action to terminate his employment.

In January 2001, Applicant started a new job. Since being hired at his new job, he has twice accessed sexually explicit internet sites without authorization on his employer's computer. He claims he has no intent to access explicit internet sites in the future.

POLICIES

The Adjudicative Guidelines in the Directive are not a set of inflexible rules of procedure. Instead they 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. In making overall common sense determinations, Administrative Judges must consider, assess, and analyze the evidence of record, both favorable and unfavorable, not only with respect to the relevant Adjudicative Guidelines, but in the context of factors set forth in section E 2.2.1. of the Directive. The government has the burden of proving any controverted fact(s) alleged in the SOR, and the facts must have a nexus to an Applicant's lack of security worthiness.

The adjudication process is based on the whole person concept. All available, reliable information about the person, past and present, is to be taken into account in reaching a decision as to whether a person is an acceptable security risk. Although the presence or absence of a particular condition for or against clearance is not determinative, the specific adjudicative guidelines should be followed whenever a case can be measured against this policy guidance.

BURDEN OF PROOF

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." As Commander in Chief, the President has "the authority to . . . control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to occupy a position . . . that will give that person access to such information." *Id.* at 527. The President has restricted eligibility for access to classified information to "United States citizens . . . whose personal and professional history affirmatively indicates loyalty to the United States, strength of character, trustworthiness, honesty, reliability, discretion, and sound judgment, as well as freedom from conflicting allegiances and potential for coercion, and willingness and ability to abide by regulations governing the use, handling, and protection of classified information." Executive Order 12968, *Access to Classified Information* § 3.1(b) (Aug. 4, 1995). Eligibility for a security clearance is predicated upon the applicant meeting the security guidelines contained in the Directive.

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, the applicant from being eligible for access to classified information. *See Egan*, 484 U.S. at 531. 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. Where the facts proven by the Government raise doubts about an applicant's judgment, reliability or trustworthiness, then the applicant has the ultimate burden of establishing his security suitability with substantial evidence in explanation, mitigation, extenuation, or refutation, sufficient to demonstrate that despite the existence of guideline conduct, it is clearly consistent with the national interest to grant or continue his security clearance.

Security clearances are granted only when "it is clearly consistent with the national interest to do so." *See* Executive Orders 10865 § 2 and 12968 § 3.1(b). "Any doubt as to whether access to classified information is clearly consistent with national security will be resolved in favor of the national security." Directive ¶ E2.2.2 "The clearly consistent standard indicates that security clearance determinations should err, if they must, on the side of denials." *See Egan*, 484 U.S. at 531. Doubts are to be resolved against the applicant.

CONCLUSIONS

The Government has satisfied its initial burden of proof under 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. E2.A13.1.1. Five times Applicant has accessed sexually explicit internet sites without authorization on his employer's computer. Disqualifying Condition 1. (E2.A13.1.2.1. *Illegal or unauthorized entry into any information technology system*) applies.

None of the Mitigating Conditions (MC) apply for the Applicant's conduct is recent with the last occurrence happening in 2002. Therefore, MC 1 (E2.A13.1.3.1. *The misuse was not recent or significant*) does not apply. MC 2 (E2.A13.1.3.2. *The conduct was unintentional or inadvertent*) does not apply because the conduct was intentional. Since there have been five incidents of misuse, MC 4 (E2.A13.1.3.4. *The misuse was an isolated event*) does not apply. C 5 (E2.A13.1.3.5. *The misuse was followed by a prompt, good faith effort to correct the situation*) does not apply because there is no showing of a good faith effort to correct the problem. What is shown is that each time Applicant's internet access was restored he returned to his misconduct.

Even with punishment becoming more severe with each incident, Applicant continued to access sexually explicit internet sites in violation of his company's rules. The first time he received a verbal warning, the second time he received a 10-day suspension, the third time, he was terminated from his job. He took voluntary retirement but knew the company would take action to terminate his employment if he did not retire. Even after losing his job, he continues to violate company rules by viewing such sites. I find against Applicant as to misuse of information technology systems.

The Government has satisfied its initial burden of proof under guideline E, (Personal Conduct). Under Guideline E, the security eligibility of an applicant is placed into question when that applicant is shown to have been involved in personal conduct which creates doubt about the person's judgment, reliability, and trustworthiness. Applicant's misuse of his computer in violation of company rules and policy is this type of conduct.

Under Guideline E personal conduct is always a security concern because it asks the central question if a person's past conduct justifies confidence the person can be trusted to properly safeguard classified information. There is evidence Applicant's wife, pastor, and friends are aware of the reasons he retired from his job, but there is no evidence they are aware he is still viewing internet sites in violation of company rules. None of the mitigating conditions apply to his personal conduct.

In reaching my conclusions I have also considered: the nature, extent, and seriousness of the conduct; the Applicant's age and maturity at the time of the conduct; the circumstances surrounding the conduct; the Applicant's voluntary and knowledgeable participation; the motivation for the conduct; the frequency and recency of the conduct; presence or absence of rehabilitation; potential for pressure, coercion, exploitation, or duress; and the probability that the circumstance or conduct will continue or recur in the future.

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: AGAINST THE APPLICANT

Subparagraph 1.a.: Against the Applicant

Subparagraph 1.b.: Against the Applicant

Subparagraph 1.c.: Against the Applicant

Subparagraph 1.d.: Against the Applicant

Paragraph 2 Personal Conduct: AGAINST THE APPLICANT

Subparagraph 2.a.: 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 or continue a security clearance for the Applicant. Clearance is denied.

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.