DATE: October 31, 2006

In Re:

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

Applicant for Security Clearance

ISCR Case No. 05-06924

DECISION OF ADMINISTRATIVE JUDGE

JOAN CATON ANTHONY

APPEARANCES

FOR GOVERNMENT

Michael Lyles, Esq., Department Counsel

FOR APPLICANT

Pro Se

SYNOPSIS

While holding an interim security clearance, and for a period of several weeks, Applicant used his employer's computers to access pornographic web sites. He was fired after his employer discovered his conduct. Applicant asserts he used his employer's computer to access and view pornography because he suffered depression caused by his work situation. Applicant has subsequently been diagnosed with Major Depressive Disorder with Seasonal Component by a psychiatrist, who has prescribed daily medication. Applicant, who continues to access pornography on his personal computer, attributes his conduct to habit. Applicant failed to mitigate Guideline M and Guideline E security concerns. Clearance is denied.

STATEMENT OF THE CASE

The Defense Office of Hearings and Appeals (DOHA) declined to grant or continue a security clearance for Applicant. On November 4, 2005, under the applicable Executive Order[(1)] and Department of Defense Directive,[(2)] DOHA issued a Statement of Reasons (SOR), detailing the basis for its decision-security concerns raised under Guideline M (Misuse of Information Technology Systems) and Guideline E (Personal Conduct)of the Directive. On November 28, 2005, Applicant answered the SOR and elected to have a hearing before an administrative judge. The case was assigned to another administrative judge on March 29, 2006. On June 20, 2006, the case was assigned to me when regional assignments were rotated.

On September 22, 2006, I convened a hearing to consider whether it is clearly consistent with the national interest to grant or continue a security clearance for Applicant. The Government called no witnesses and introduced five exhibits, which were identified and numbered Ex. 1 through 5. The Government withdrew Ex. 5 as redundant. The remaining Government exhibits were admitted without objection. Applicant called one witness and introduced three exhibits, which were identified as Exs. A, B, and C, and admitted without objection. At the conclusion of the evidence, I left the record open until October 2, 2006, so that Applicant could, if he wished, submit a letter from his psychiatrist specifying his diagnosis and treatment. Applicant timely filed such a letter, which was identified as Applicant's Ex. D and entered

in the record without objection. DOHA received the transcript (Tr.) of the proceeding on October 3, 2006.

FINDINGS OF FACT

The SOR in this case contains one allegation of disqualifying conduct under Guideline M, Misuse of Information Technology Systems, and one allegation of disqualifying conduct under Guideline E, Personal Conduct. In his answer to the SOR, Applicant admitted the two allegations. His admissions are incorporated as findings of fact.

Applicant will be 33 years old in December 2006. He graduated from college in 2001 with a bachelor of science degree in aerospace engineering. He has been employed since January 2005 as an applications engineer by a government contractor. (Tr. 54; Ex. 1, Ex. A.) Applicant has been married for approximately five years. He and his wife met while in college. (Tr. 42, 44-45.)

Applicant was hired by Employer A in August 2001 as an engineer/scientist 1. He worked for his employer for two years at two job sites in State B. After two years, Applicant transferred to another division within Employer A's company and took a position identified as flight engineer.

Applicant's position as flight engineer required that he transfer to a work site and to a project in another part of the U.S. His employer also required that he apply for a security clearance. He was assigned to work temporarily in State C and to wait there until assigned to the work site in State D. Applicant's wife accompanied him to State C. The couple arrived in State C in the latter part of July 2003. (Tr. 52.) While on the temporary assignment, Applicant's household goods were placed in storage, and he and his wife lived in a hotel. He received his regular salary of approximately $53,000 per annum and per diem. (Tr. 72-73.) When he arrived in State C, Applicant was informed he had been granted a security clearance. (Ex. 3; Tr. 61-62.)

When Applicant began working for Employer A in State C, he was assigned to the first shift, where he worked for approximately three weeks. On one occasion, after the other first shift employees had left for the day, Applicant stayed at work and accessed pornographic web sites on the computer assigned to him by Employer A. (Ex. 2 at 8.)

Applicant's supervisor, who was not aware Applicant had accessed pornographic web sites during the first shift, then asked him to work the second shift in order to fill in for an employee on vacation. Applicant was assigned to the second shift from August 22, 2003 through September 26, 2003. He found he was able to complete his regularly assigned second shift work in about two hours. He was then assigned to stand by to sign off on aircraft maintenance issues. Applicant worked alone for several hours during the second shift. He spent three to four hours a night surfing the Internet. That activity included accessing pornographic sites when no other employees were in the work area. (Ex. 2 at 8; Tr.58-60.)

During the period beginning August 22, 2003, and ending September 26, 2003, Applicant used two computers in his work area to access pornographic material. (Ex. 2 at 2-7.) After returning to first shift work, Applicant stayed after work and continued to access pornographic web sites when the other employees had left for the day. (Tr. 60-61.)

Employer A initiated an investigation of computer access when an audit of the company's "access denied" report for September 2003 indicated an unusually high number of denials to web sites considered inappropriate for the workplace. An internal investigation identified Applicant as the person accessing pornographic sites. He was interviewed and signed a statement admitting using his employer's computers to access pornographic material and acknowledging his actions were against company policy. (Ex. 2 at 8-9.) On December 10, 2003, Employer A issued an Employee Corrective Action Memo to Applicant. In pertinent part, the Memo read::

You have used [Company A's]-provided computer workstations to access, and/or attempt to access, non-work related, restricted and inappropriate websites, and you have mischarged your labor time while performing these activities during your normal work hours.

You will be discharged from [Company A] effective Thursday, 11 December 2003 (last day on payroll).

(Ex. 4 at 2, 3.)

In explanation, Applicant stated he and his wife felt considerable stress while in State C because they didn't know when they would be leaving to live in State D. They had expected to stay in State C for about one week and then transfer to State D. Instead, his assignment to the company's facility in State C lasted for 2 ½ months. During that time, Applicant's wife became ill with gall bladder problems. Applicant suggested the stresses he and his wife experienced caused him to be depressed and to seek pornography to relieve his stress. (Tr. 31-33.)

Applicant has been under treatment by a psychiatrist for approximately eighteen months. He was diagnosed with Major Depressive Disorder with Seasonal Component. He takes daily medication for depression, and he consults with his doctor every three months. He believes his depression is under control. (Tr. 64-65, 77; Ex. D.) He currently accesses pornographic material on his home computer. He thinks his use of pornographic material might be related to habit. (Tr. 70-72.)

Applicant took responsibility for his conduct and did not attempt to hide it from his family or on his security clearance application. (Ex. 1; Tr. 18-19; 29-31; 39-41.) His current employer praises Applicant's professional work ethic and his dedication to his job. His performance review for the period January 17, 2005 to January 16, 2006 indicates he exceeds expectations on all job review elements. (Ex. A, B, C.)

POLICIES

"[N]o one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988). 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." Exec. Or. 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.

Enclosure 2 of the Directive sets forth personal security guidelines, as well as the disqualifying conditions and mitigating conditions under each guideline. In evaluating the security worthiness of an applicant, the administrative judge must also assess the adjudicative process factors listed in ¶ 6.3 of the Directive. The decision to deny an individual a security clearance is not necessarily a determination as to the loyalty of the applicant. *See* Exec. Or. 10865 § 7. It is merely an indication that the applicant has not met the strict guidelines the President and the Secretary of Defense have established for issuing a clearance.

Initially, the Government must establish, by substantial evidence, conditions in the personal or professional history of the applicant that disqualify, or may disqualify, the applicant from being eligible for access to classified information. *See Egan*, 484 U.S. at 531. The Directive presumes a nexus or rational connection between proven conduct under any of the disqualifying conditions listed in the guidelines and an applicant's security suitability. *See* ISCR Case No. 95-0611 at 2 (App. Bd. May 2, 1996).

Once the Government establishes a disqualifying condition by substantial evidence, the burden shifts to the applicant to rebut, explain, extenuate, or mitigate the facts. ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002); *see* Directive ¶ E3.1.15. An applicant "has the ultimate burden of demonstrating that it is clearly consistent with the national interest to grant or continue his security clearance." ISCR Case No. 01-20700 at 3.

CONCLUSIONS

Guideline M - Misuse of Information Technology Systems

In the SOR, DOHA alleged under Guideline M of the Directive that Applicant was fired from his job with Employer A after an investigation revealed he had accessed sexually explicit internet sites without authorization on two of his

employer's computers, knowing that such access was non-work related, restricted, and inappropriate. Additionally, DOHA alleged Applicant mischarged his labor time while performing these unauthorized activities during normal work hours, conduct that was specifically prohibited by company rules, procedures, and guidelines.(¶ 1.a.)

Applicant's many unauthorized entries into his employer's technology system during at least August and September 2003 violated his employer's policy and procedures. Applicant's conduct raises security concerns under Disqualifying Condition (DC) E2.A.13.1.2.1. of Guideline M. Three years have passed since Applicant misused his employer's computer system, and thus his misuse was not recent. However, the misuse was significant. The record evidence and Applicant's credible testimony indicate his misuse of his employer's computer system was knowing and deliberate. His misuse of his employer's information technology system occurred repeatedly over a period of several weeks and was not limited to isolated events. Accordingly, while Mitigating Condition (MC) E2.A.13.1.3.1. applies in part, MC E2.A.13.1.3.2. and MC E2.A.13.1.3.4. are inapplicable to the facts of Applicant's case.[(3)]

Additionally, MC E2.A13.1.3.5. does not apply to Applicant's case, since his misuse was carried out surreptitiously and was not followed by a prompt, good faith effort to correct the situation.[(4)] I conclude that Applicant has failed to mitigate the disqualifying conduct alleged in ¶ 1.a. of the SOR

Guideline E - Personal Conduct

In the SOR, DOHA alleged under Guideline E that Applicant misused his employer's information technology system as alleged in ¶ 1.a. and that the misuse reflected questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty or unwillingness to comply with rules and regulations and further suggested Applicant may not properly safeguard classified information. (¶2.a.)

Guideline E conduct raises security concerns because it involves questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations and could indicate that an applicant may not properly safeguard classified information. Directive ¶ E2.A5.l.l.

Applicant's conduct raises security concerns under three Disqualifying Conditions (DC) under Guideline E. First, reliable, unfavorable information about Applicant's alleged unprofessional conduct and questionable judgment was provided by his employer, raising a concern under DC E2.A5.1.2.1. of the Guideline. Second, Applicant's alleged personal conduct, which included the secretive misuse of his employer's computer system to access pornographic material, increased his vulnerability to coercion, exploitation, or duress, raising a concern under DC E2.A5.1.2.4. Third, Applicant's alleged disqualifying personal conduct reflected a pattern of dishonesty or rule violations, raising a concern under DC E2.A5.1.2.5.

We turn to an examination of possible Mitigating Conditions (MC) under the Guideline. The information about Applicant's unprofessional conduct that was provided by his employer is pertinent to a determination of his judgment, trustworthiness, or reliability. Therefore, MC E2.A5.1.3.1 is inapplicable. At his hearing, Applicant provided evidence he had sought psychiatric treatment for his depression, a condition he said caused him to access pornographic material. However, he also provided evidence that even after treatment, he continued to access pornography, albeit privately and legally on his personal computer, out of habit, thus raising the issue of continued vulnerability to coercion, exploitation, or duress. Accordingly, MC E2.A5.1.3.5. is inapplicable, and the Guideline E allegation of the SOR is concluded against Applicant.

In my evaluation of the record, I have carefully considered each piece of evidence in the context of the totality of evidence and under all the Directive guidelines that were generally applicable or might be applicable to the facts of this case. Under the whole person concept, as specified at ¶ E2.2.of Enclosure 2 of the Directive, I conclude Applicant has failed to rebut or mitigate the Government's case opposing his request for a DoD security clearance.

FORMAL FINDINGS

The following are my conclusions as to the allegations in the SOR:

Paragraph 1.: Guideline M: AGAINST APPLICANT

Subparagraph 1.a.: Against Applicant

Paragraph 2.: Guideline E: AGAINST APPLICANT

Subparagraph 2.a.: Against Applicant

DECISION

In light of all of 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 Applicant. Clearance is denied.

Joan Caton Anthony

Administrative Judge

1. Exec. Or. 10865, *Safeguarding Classified Information within Industry* (Feb. 20, 1960), as amended and modified.

2. Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (Jan. 2, 1992), as amended and modified.

3. MC E2.A13.1.3.1.reads: The misuse was not recent or significant. MCE2.A13.1.3.2. reads: The conduct was unintentional or inadvertent. MC E2.A13.1.3.4. reads: The misuse was an isolated event.

4. MC E2.A13.1.3.5.reads: The misuse was followed by a prompt, good faith effort to correct the situation.