KEYWORD: Personal Conduct

DIGEST: Applicant was a project manager for a computer service company working on defense contracts. Hundreds of times over approximately a two month period, he accessed and downloaded from the Internet pornographic images using the company computer network in violation of company policy. Clearance is denied.

CASENO: 03-15308.h1

DATE: 03/04/2005

DATE: March 4, 2005

In Re:

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

Applicant for Security Clearance

ISCR Case No. 03-15308

DECISION OF ADMINISTRATIVE JUDGE

THOMAS M. CREAN

APPEARANCES

FOR GOVERNMENT

Stephanie C. Hess, Esq., Department Counsel

Candace Le'I, Esq., Department Counsel

FOR APPLICANT

Pro Se

SYNOPSIS

Applicant was a project manager for a computer service company working on defense contracts. Hundreds of times over approximately a two month period, he accessed and downloaded from the Internet pornographic images using the company computer network in violation of company policy. Clearance is denied.

STATEMENT OF THE CASE

On July 16, 2004, the Defense Office of Hearing and Appeals (DOHA) issued a Statement of Reasons (SOR) detailing the basis for its decision to not grant a security clearance to Applicant. The action was taken under Executive Order 10865, *Safeguarding Classified Information within Industry* (February 20, 1990), as amended and modified, and Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended and modified (Directive). Applicant acknowledged receipt of the SOR on August 2, 2004. The SOR alleges security concerns under Guideline E (Personal Conduct) of the Directive.

Applicant answered the SOR in writing on August 2, 2004. His answers were not complete and on August 12, 2004, DOHA requested a complete response. Applicant provide a complete response in writing on August 20, 2004, denying the allegation under Guideline E and providing an explanation for his actions. He requested a hearing before an administrative judge. The request for a hearing was received by DOHA on August 23, 2004. Department Counsel was prepared to proceed with the case on December 7, 2004, and the case was assigned to me on December 9, 2004. A notice of hearing was issued on January 5, 2005, and the hearing was held on February 9, 2005. Four government exhibits, five Applicant exhibits, and the testimony of the Applicant were received during the hearing. The transcript was received on February 17, 2005.

FINDINGS OF FACT

Applicant is a 63-year-old executive for a small technology company which does some work for the Department of Defense. Previously, Applicant was a project manager for a large computer services company doing work as a defense contractor. He is married for over 35 years and has three grown children. He worked in the computer service business for over 40 years and worked for the defense contractor computer service company for over 21 years. He held a security clearance from various government agencies for over 30 years.[(1)]

In late 2001, Applicant's employer learned through their software program monitoring its computer network that Applicant had been accessing and downloading pornographic material using his office computer. Because of problems with use of the network, the company had established a policy, and notified its employees, that the office computer network should not be used to access and download non-business related information. The company's review of Applicant's computer usage revealed the pornographic access and downloads. Some of the downloaded images appeared to be

child pornography. Applicant was terminated for violation of company policy.[(2)] Applicant's employer changed the nature of his termination to permit him to draw state unemployment benefits.[(3)]

The pornographic material was accessed using the company network through Applicant's personal internet service provider account. He discovered on his home computer that his son or another person had established access from the internet service provider account to "Newsgroups", some of which provided access to pornographic images. About October 1, 2001, Applicant started using his office computer to access these sites. He looked at these images hundreds of times over the next 45 to 60 days. When Applicant accessed an image, it automatically downloaded to his office network because of the operating requirements of the internet service provider and his office network.[(4)]

Applicant denied knowledge of a company change in policy concerning accessing and downloading information on the Internet using the company network. He received many memorandum and e-mails from company management, especially the human resource department, and did not read them all and ignored many. Applicant was in management meetings that discussed the policy of limiting use of the company network. Applicant knew companies normally limit their employees use of the internet so as to preserve company computer capabilities. As a company manager and computer expert, he counseled employees under his supervision about use of the company network. Applicant did use the network for authorized business purposes to access on the Internet computer operating news, to include AOL news groups, that were of business interest to his employees.[(5)]

Applicant blamed his firing on a personal conflict with the company's human resources director. When his downloading of the images was discovered, Applicant's supervisor wanted to retain him but the human resources director wanted him terminated. Applicant attributed this to their personal conflicts and the desire to downsize the company and not pay severance bonuses. Prior to the incident, Applicant had received excellent performance ratings.[(6)]

POLICIES

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."[(7)] 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 judgement, 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."[(8)] Eligibility for a security clearance is predicated upon the applicant meeting the security guidelines contained in the Directive.

The Directive sets out the adjudicative guidelines for making decisions on security clearances. Enclosure 2 of the Directive sets forth adjudicative guidelines for determining eligibility for access to classified information, and it lists the disqualifying conditions (DC) and mitigating conditions (MC) for each guideline. Each clearance decision must be fair, impartial, and a commonsense decision based on the relevant and material facts and circumstances, the whole person concept, and the factors listed in the Directive ¶ 6.3.1 through ¶ 6.3.6

"The adjudicative process is an examination of a sufficient period of a person's life to make an affirmative determination that the person is eligible for a security clearance."[(9)] An administrative judge must apply the "whole person concept," and consider and carefully weigh the available, reliable information about the person.[(10)] An administrative judge should consider: (1) the nature, extent, and seriousness of the conduct; (2) the circumstances surrounding the conduct, to include knowledgeable participation; (3) the frequency and recency of the conduct; (4) the applicant's age and maturity at the time of the conduct; (5) the voluntariness of participation; (6) the presence or absence of rehabilitation and other pertinent behavioral changes; (7) the motivation for the conduct; (8) the potential for pressure, coercion, exploitation, or duress; and (9) the likelihood of continuation of recurrence.[(11)]

A person granted access to classified information enters into a special relationship with the government. The government must be able to repose a high degree of trust and confidence in those individuals to whom it grants access to classified information. The decision to deny an individual a security clearance is not necessarily a determination as to the loyalty of the applicant.(12) 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 present evidence to establish controverted facts in the SOR that disqualify or may disqualify the Applicant from being eligible for access to classified information.(13) Thereafter, Applicant is responsible for presenting evidence to rebut, explain, extenuate, or mitigate facts.(14) An applicant "has the ultimate burden of demonstrating that it is clearly consistent with the national interest to grant or continue his security clearance."(15) " [T]he Directive presumes there is a nexus or rational connection between proven conduct under any of the Criteria listed therein and an applicant's security suitability."(16) "Any doubt as to whether access to classified information is clearly consistent with national security will be resolved in favor of the national security." (17)

CONCLUSIONS

I carefully considered all of the facts in evidence and the legal standards discussed above. I reach the following conclusions regarding the allegations in the SOR:

Under Guideline E (Personal Conduct), a security concern exists for conduct involving questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations. Any of these characteristics in a person could indicate that the person may not properly safeguard classified information.(18) Applicant's conduct in accessing and downloading pornographic material from the Internet in violation of company policy brings the matter under Personal Conduct Disqualifying Condition E2.A5.1.2.5 (*a pattern of dishonesty or rules violation,. . .*). Over a period of 45 to 60 days, Applicant admitted to repeatedly accessing and downloading pornographic material using his company computer which violated company policy. Applicant's repeated conduct over a period of time is a pattern of dishonesty or rules violation. I conclude the Personal Conduct Disqualifying Condition has been established.

Applicant has not established any of the mitigating conditions under Guideline E.(19) He admits to knowing the underlying company policy of not using the company computer network to access non-business related information. His excuse that he did not receive the policy change from the human resources department is disingenuous. He was a company manager and had participated in meetings in which the policy concerning use of the network was discussed. He blames his termination on his conflict with the human resources director. The real issue is not his termination but the violation of company policy by accessing and downloading pornographic images using the company's computer

network. He readily admitted to this conduct of downloading the material and did not provide any information to mitigate this conduct.

I carefully considered all of the circumstances in light of the "whole person" concept for a fair, impartial, and commonsense decision. I conclude Applicant is not eligible for access to classified information.

FORMAL FINDINGS

Formal findings for or against Applicant on the allegation set forth in the SOR, as required by Section E3.1.25 of Enclosure 3 of the Directive, is:

Paragraph 1, Guideline E: AGAINST APPLICANT

Subparagraph 1.a.: Against Applicant

DECISION

In light of all of the circumstances presented in 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.

Thomas M. Crean

Administrative Judge

1. Tr. 21-22.

2. Government Exhibit 3 (Letter to Defense Security Service, dated January 3, 2002); Government Exhibit 4 (Memorandum from Company Human Resources Director, dated December 20, 2001); Tr. 21-22.

3. Applicant Exhibit E (Applicant's letter to Department Counsel, dated February 15, 2005). This letter was received after the hearing and Department Counsel had no objection to admitted it into the record as Applicant Exhibit E. Applicant inadvertently forgot to have it admitted at the hearing.

4. Government Exhibit 2 (Applicant's statement, dated December 4, 2002) at 3; Tr. 27-30.

5. Tr. 34-40.

6. Applicant Exhibit B (Performance rating, dated April 1, 2001); Applicant Exhibit C (Performance rating, dated May 19, 2000); Applicant Exhibit D (Performance rating, dated April 5, 1999).

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

8. Exec. Or. 12968, *Access to Classified Information* § 3.1 (b) (Aug. 4, 1995).

9. Directive ¶ E2.2.1.

10. *Id.*

11. Directive ¶¶ E2.2.1.1 through E2.2.1.9.

12. *See* Exec. Or. 10865 § 7.

13. Directive ¶ E3.1.14.

14. ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002); *see* Directive ¶ E3.1.15.

15. ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002).

16. ISCR Case No. 95-0611 at 2 (App. Bd. May 2, 1996) (quoting DISCR Case No. 92-1106 (App. Bd. Oct. 7, 1993))

17. *Egan,* 484 U.S. at 531; *see* Directive ¶ E2.2.2.

18. Directive ¶ E2.A5.1.1.

19. Directive ¶ E2.A5.1.3.