DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
----------	)	ISCR Case No. 08-04593
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Jeff A. Nagel, Department Counsel
For Applicant: Alan V. Edmunds, Attorney At Law

April 24, 2012

Decision

LOKEY ANDERSON, Darlene D., Administrative Judge:

Applicant submitted his Electronic Questionnaire for Investigations Processing (e-QIP) dated April 30, 2008. (Government Exhibit 1.) On October 28, 2010, the Defense Office of Hearings and Appeals (DOHA), pursuant to Executive Order 10865 (as amended), and Department of Defense Directive 5220.6 (Directive), dated January 2, 1992, issued a Statement of Reasons (SOR) to the Applicant, which detailed the reasons why DOHA could not make the preliminary affirmative finding under the Directive that it is clearly consistent with the national interest to grant or continue a security clearance for the Applicant and recommended referral to an Administrative Judge to determine whether a clearance should be denied or revoked.

The Applicant responded to the SOR on November 16, 2010, and he requested a hearing before a DOHA Administrative Judge. This case was assigned to another undersigned Administrative Judge on November 7, 2011. A notice of hearing was issued that same day, scheduling the hearing for December 13, 2011. The Government presented seven exhibits, referred to as Government Exhibits 1 through 7, which were admitted without objection. The Applicant presented twelve exhibits, referred to as

Applicant's Exhibits A through L, which were admitted without objection. At this point, it was determined that the assigned Administrative Judge had been a Department Counsel on a companion case concerning this matter. Both the current assigned Department Counsel and the Applicant's attorney voir dired the Judge and both parties moved to have the Judge excused from the matter. The case was re-assigned to the undersigned Administrative Judge on January 4, 2012. The case was set on February 8, 2012, for hearing on February 27, 2012, by video-teleconference. The Government's seven exhibits and the Applicant's twelve exhibits were reintroduced into the record. The Applicant called three witnesses and testified on his own behalf. The official transcripts (Tr.) were received on December 21, 2011 and March 13, 2012. Based upon a review of the pleadings, exhibits, and testimony, eligibility for access to classified information is granted.

FINDINGS OF FACT

The following Findings of Fact are based on the Applicant's Answer to the SOR, the testimony and the exhibits. The Applicant is 42 years old, and has a Bachelor's Degree in Computer Science, and is currently finishing up his last semester toward his Master's Degree. He is employed by a defense contractor as a Software Engineer and is seeking to obtain a security clearance in connection with his employment.

The Government opposes the Applicant's request for a security clearance, on the basis of allegations set forth in the Statement of Reasons (SOR). After a complete and thorough review of the evidence in the record, and upon due consideration of the same, the following findings of fact are entered as to each paragraph and guideline in the SOR:

Paragraph 1 (Guideline E - Personal Conduct). The Government alleges that the Applicant is ineligible for a security clearance because he engaged in conduct which shows questionable judgment, lack of candor, dishonesty or unwillingness to comply with rules and regulations .

Paragraph 2 (Guideline M - Use Information Technology Systems).
The Government alleges that the Applicant is ineligible for a security clearance due to his noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems calling into question his willingness or ability to properly protect sensitive systems, networks, and classified information.

The Applicant was terminated from employment from three separate companies during the period from 2000 to 2005, for violating rules and regulations, namely for the misuse of government or company property, specifically information technology systems, and for unsatisfactory performance. The details concerning these terminations are set forth below:

In September 2005, the Applicant was working for a defense contractor. After lodging an anonymous complaint by e-mail against the Security Director, because he felt someone was unjustly terminated, (and which given its nature could be interpreted as threatening management), the Applicant was told not to come to work and was placed on a two week suspension. During his suspension, the Security Director ordered a forensic investigation of the Applicant's work computer. The computer was located in the Applicant's locked and access-controlled protected office. The investigation revealed that the Applicant had accessed pornographic web sites and pornographic photos on his government computer during work hours. The Applicant testified that during his employment there, he received numerous e-mails that contained adult pornography. He typically opened up and viewed the adult sex and pornographic e-mails and photographs during work hours, knowing that he was not authorized to do so. (Tr. p. 59.) He testified that the longest single visit to an adult website was 33 minutes. (Government Exhibit 4.)

The forensic report of the Applicant's computer revealed pornographic photographs, camera view (live web cam video), storage of pornographic materials, transmittal of pornographic photographs and materials using his government e-mail account and storage and transmittal of pornographic photos. (Government Exhibits 5 and 6.)

The Applicant acknowledged that he was told that while in suspension, he was not to access his office or his computer, but that he was never told that he could not come in the building. In direct violation of this order, during his suspension, he gained access to the building after hours, during the weekend to get his checkbook, and to check his e-mail in his office. At that time, he e-mailed some non-work related matters to his home. (Tr. p. 63.) . The investigation found that the Applicant had logged into the system using his password to try to scrub the computer. It also revealed that the Applicant had personal information on his sensitive computer including his bank information, an ebay, and amazon account, and a quicken bill pay program, among others. The Applicant states since his security access card was not turned off, nor was he placed on a list at the front desk of people not allowed in the building he did not see a problem with it. (Tr. p. 87 and Government Exhibit 4.)

The Applicant knowingly violated his company's "zero tolerance policy" regarding viewing pornographic web sites. He admits to viewing pornography at work on his work computer. (Tr. p. 75.) In retrospect, he realizes that this was a huge mistake. He testified that in the future, he will never look at pornographic material at work or on a work computer. (Tr. p.73.) The Applicant contends that his work computer was unclassified, not on the government network and did not compromise government security. It was however viewed on a sensitive government computer. As a result of this misconduct, the Applicant was terminated from his job position. (Tr. p. 95.)

In 2001, the Applicant was working for a small start up company. As the company grew, there were strong differences of opinion on the direction of the company concerning design and architecture matters. The Applicant described it as a "big blow

up" and he was fired. (Tr. p. 79.) The Applicant was terminated from employment due to unsatisfactory performance. (Tr. p. 95.)

In 2000, the Applicant was working for a defense contractor by day and moonlighting by night. During the day, if he had some down time, he would work on his outside work. Through routine computer scans, the company found some of the Applicant's outside work on his day work computer. The Applicant was terminated from employment for his misuse of information technology resources. (Tr. p. 95.)

The Applicant testified that he did not reveal his past employment terminations to his present employer because he was not asked about them. He explained that during his hiring process he underwent a technical interview and was asked about the technologies he uses and the projects he worked on. He was not asked why he left his past employment. (Tr. pp. 70 -71.)

Three witnesses testified on behalf of the Applicant, including his supervisor, a coworker and past office mate, and a friend and past coworker. They consider the Applicant to be a trustworthy individual who simply made a mistake in the past. They testified that if they received pornographic e-mails on their work computer they would have deleted them and/or reported it to company security. (Tr. pp. 16-21, 37-43, and 100-104.)

Letters of recommendation submitted by both professional and personal associates of the Applicant, including the Facility Security Manager, attest to the Applicant's responsible, trustworthy, and professional nature. He is said to demonstrate a strong work ethic, honesty and integrity. He is a top and valued performer of the company and highly regarded. He is recommended for a security clearance. (Applicant's Exhibits E, F, G, H, I, J, K and L.)

The Applicant received an award when he was a summer hire computer clerk, from the Department of the Army for his contribution to the Quality and Instrumentation Engineering Branch during the period from July 7,1991, through July 19, 1991 He received an On-the-Spot Cash award of $1,000.00. (Applicant's Exhibit D.)

POLICIES

Enclosure 2 of the Directive sets forth adjudication policies divided into "Disqualifying Factors" and "Mitigating Factors." The following Disqualifying Factors and Mitigating Factors are found to be applicable in this case:

Guideline E (Personal Conduct)

15. *The Concern*. Conduct involving questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations can raise questions about an individual's reliability, trustworthiness and ability to protect classified

information. Of special interest is any failure to provide truthful and candid answers during the security clearance process or any other failure to cooperate with the security clearance process.

Condition that could raise a security concern:

16.(c) credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any other single guideline, but which when considered as a whole, supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the person may not properly safeguard protected information.

Condition that could mitigate security concerns:

17.(d) the individual has acknowledged the behavior and obtained counseling to change the behavior or taken other positive steps to alleviate the stressors, circumstances, or factors that caused untrustworthy, unreliable, or other inappropriate behavior, and such behavior is unlikely to recur.

Guideline M (Use of Information Technology Systems)

39. The Concern. Noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual's reliability and trustworthiness, calling into question the willingness or ability to properly protect sensitive systems, networks and information. Information technology systems include all related computer hardware, software, firmware, and date used for the communication, transmission, processing, manipulation, storage, or protection of information.

Conditions that could raise a security concern:

40.(a) illegal or unauthorized entry into any information technology system or component thereof;

40.(e) unauthorized use of a government or other information technology system.

Condition that could mitigate security concerns:

41.(a) so much time has elapsed since the behavior happened, or it happened under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment.

In addition, as set forth in Enclosure 2 of the Directive at pages 18-19, in evaluating the relevance of an individual's conduct, the Administrative Judge should consider the following general factors:

a. The nature, extent, and seriousness of the conduct;

b. The circumstances surrounding the conduct, to include knowledgeable participation;

c. The frequency and recency of the conduct;

d. The individual's age and maturity at the time of the conduct;

e. The extent to which participation is voluntary;

f. The presence or absence of rehabilitation and other permanent behavioral changes;

g. The motivation for the conduct;

h. The potential for pressure, coercion, exploitation or duress; and

i. The likelihood of continuation or recurrence.

The eligibility criteria established in the DoD Directive identify personal characteristics and conduct which are reasonably related to the ultimate question, posed in Section 2 of Executive Order 10865, of whether it is "clearly consistent with the national interest" to grant an Applicant's request for access to classified information.

The DoD Directive states, "The adjudicative process is an examination of a sufficient period of a person's life to make an affirmative determination that the person is an acceptable security risk. Eligibility for access to classified information is predicated upon the individual meeting these personnel security guidelines. The adjudicative process is the careful weighing of a number of variables known as the whole person concept. Available, reliable information about the person, past and present, favorable and unfavorable should be considered in reaching a determination." The Administrative Judge can draw only those inferences or conclusions that have reasonable and logical basis in the evidence of record. The Judge cannot draw inferences or conclusions based on evidence which is speculative or conjectural in nature. Finally, as emphasized by President Eisenhower in Executive Order 10865, "Any determination under this order . . . shall be a determination in terms of the national interest and shall in no sense be a determination as to the loyalty of the Applicant concerned."

CONCLUSIONS

In the defense industry, a security clearance is entrusted to civilian workers who must be counted upon to safeguard such sensitive information twenty-four hours per day, seven days per week. The Government is therefore appropriately concerned when available information indicates that an Applicant for such access may be involved in

instances of financial irresponsibility and misconduct, which demonstrates poor judgment or unreliability.

It is the Government's responsibility to present substantial evidence to support the finding of a nexus, or rational connection, between the Applicant's conduct and the holding of a security clearance. If such a case has been established, the burden then shifts to the Applicant to go forward with evidence in rebuttal, explanation or mitigation which is sufficient to overcome or outweigh the Government's case. The Applicant bears the ultimate burden of persuasion in proving that it is clearly consistent with the national interest to grant him a security clearance.

In this case the Government has met its initial burden of proving that the Applicant has engaged in poor personal conduct (Guideline E), and that he engaged in the misuse of information technology systems (Guideline M). This evidence indicates poor judgment, unreliability and untrustworthiness on the part of the Applicant. Because of the scope and nature of the Applicant's conduct, I conclude there is a nexus or connection with his security clearance eligibility.

The evidence shows that during a five year period from 2000 to 2005, the Applicant was terminated from three places of employment for failing to comply with company rules and regulations regarding either the unauthorized and misuse of the government and/or company computer, and for unsatisfactory performance. The e-mail in question that was sent by the Applicant is disturbing. From the evidence presented, it appears that the Applicant was at one time a hot head who did what he wanted to do, regardless of the consequences. His disruptive workplace behavior, statements of bitterness, resentment, disgruntlement, argumentative nature and numerous disagreements with his company management proved difficult to deal with and for some became intolerable. His inappropriate conduct during that period of time clearly exhibited immaturity, ignorance, poor judgment and lack of professionalism.

Over the past seven years, I believe the Applicant has significantly grown up. He now appears to realize his serious mistakes of the past. He understands the importance and the responsibilities associated with holding a security clearance and has convinced me that he will never engage in this kind of inappropriate activity at work in the future. He understands that government and company computers are reserved for just that, nothing more. He understands that if he is to view pornography, it had better be done in the privacy of his own home on his own personal computer. I believe he also realizes the importance of getting along with his management and maintaining a professional attitude at all times, whether he disagrees with them or not.

Although the Applicant did not reveal his past three job terminations to his present employer, it appears that he was not asked about them. During his hiring process, his employer was more concerned about his technical skills and the contribution he could make to the company. Under these circumstances, I cannot find that he intentionally or deliberately failed to disclose the information, or that he wrongfully concealed it. However, for future matters, the Applicant must be open, up

front and candid with his past employment history if he is to continue working in the defense industry with a security clearance.

Under Guideline E, the Applicant's poor personal conduct reflects negatively on his ability to be trusted with the national secrets. The Applicant's pattern of misconduct involving rule violations demonstrates poor judgment, unreliability and untrustworthiness. However, it occurred over seven years ago and there has been no reoccurrence. The Applicant acknowledges his mistakes, and indicates that he has changed his ways.

Disqualifying Condition 16.(c) *credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any other single guideline, but which when considered as a whole, supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the person may not properly safeguard protected information* applies. Mitigating Condition 17.(d) *the individual has acknowledged the behavior and obtained counseling to change the behavior or taken other positive steps to alleviate the stressors, circumstances, or factors that caused untrustworthy, unreliable, or other inappropriate behavior, and such behavior is unlikely to recur* also applies

Turning to Guideline M, the Applicant's misuse of the government and/or company computer by viewing pornography at work, during work hours is inexcusable and demonstrates extremely poor judgment, unreliability and untrustworthiness. Disqualifying Conditions 40.(a) *illegal or unauthorized entry into any information technology system or component thereof*, and 40.(e) *unauthorized use of a government or other information technology system* apply. Mitigating Condition 41.(a) *so much time has elapsed since the behavior happened, or it happened under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment* also applies.

I have also considered the "whole-person concept" in evaluating the Applicant's eligibility for access to classified information, including witness testimony and his favorable letters of recommendation. Under the particular facts of this case, the totality of the conduct set forth under all of the guidelines viewed as a whole, support a whole person assessment of good judgement, trustworthiness, reliability, candor, a willingness to comply with rules and regulations, or other characteristics indicating that the person may properly safeguard classified information.

On balance, it is concluded that the Applicant has overcome the Government's case opposing his request for a security clearance. Accordingly, the evidence supports a finding for the Applicant as to the factual and conclusionary allegations expressed in Paragraphs 1 and 2 of the Government's Statement of Reasons.

FORMAL FINDINGS

Formal findings For or Against the Applicant on the allegations in the SOR, as required by Paragraph 25 of Enclosure 3 of the Directive are:

Paragraph 1: For the Applicant.
Subpara. 1.a.: For the Applicant.
Subpara. 1.b.: For the Applicant.

Paragraph 2: For the Applicant.
Subpara. 2.a.: For the Applicant.

DECISION

In light of the circumstances presented by the record in this case, it is clearly consistent with the national interests to grant or continue a security clearance for the Applicant.

Darlene Lokey Anderson
Administrative Judge