DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ADP Case No. 07-18446
SSN:	)	
	)	
Applicant for Public Trust Position	)	

Appearances

For Government: James Duffy, Esquire, Department Counsel
For Applicant: Pro Se

March 18, 2009

Decision

HOGAN, Erin C., Administrative Judge:

Applicant submitted a Public Trust Position Application (SF 85P) on March 6, 2006. On August 13, 2008, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) detailing the trustworthiness concerns under Guideline M, Use of Information Technology Systems, and Guideline E, Personal Conduct for Applicant. The action was taken under Executive Order 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive), and the revised adjudicative guidelines (AG) promulgated by the President on December 29, 2005, and effective within the Department of Defense for SORs issued after September 1, 2006.

On September 15, 2008, Applicant answered the SOR and requested a hearing before an Administrative Judge. Department Counsel was prepared to proceed on November 17, 2008. The case was assigned to another administrative judge on November 17, 2008. The case was transferred to me on December 12, 2008. On February 6, 2009, a Notice of Hearing was issued scheduling the hearing for February 23, 2009. The hearing was held as scheduled. The Government called two witnesses and offered three exhibits which were admitted as Government Exhibits (Gov) 1 – 3, without objection. Applicant testified, called two witnesses and offered two exhibits

which was admitted as Applicant Exhibits (AE) A and B. DOHA received the transcript of hearing on March 3, 2009. Based upon a review of the case file, pleadings, exhibits, and testimony, eligibility for access to position of public trust is granted.

Findings of Fact

In his Answer to the SOR, Applicant admits the allegation in SOR ¶ 1.a, but denies the allegations in SOR ¶¶ 2.a and 2.b.

Applicant is a 51-year-old senior technology architect employed with a Department of Defense contractor seeking a position of public trust. He has been employed with the defense contractor since May 2005. He is married and has an 18-year-old son and a sixteen-year-old stepson. He has a bachelor's degree in aeronautical and astronautical engineering and has taken some graduate level courses. He has held some form of a security clearance or position of public trust since 1982. (Tr at 5-7, 15-16, 93; Gov 1)

From January 1981 to February 2005, Applicant was employed with another defense contractor. His last position with the contractor was senior staff engineer. His employer issued him a laptop computer for him to use in order to fulfill his duties. He was authorized to take the laptop with him when he traveled for the company. Applicant traveled quite often. (Tr at 15-16, 93)

Applicant's previous employer had rules which prohibited the use of company computers to visit pornographic and/or adult websites. The rules also prohibited the use of the company computer to view pornographic pictures and/or download pornographic videos. Applicant admits that he was aware of the above company rules. He signed a statement acknowledging that he was aware of the rules pertaining to the proper use of the computer. (Tr at 16-17) The Manager of the company's Security Operations and Investigations Department, stated the rules prohibiting the use of company computers to access pornography was widely known by all of the company's employees. (Tr at 44)

From August 2004 to July 2005, Applicant was assigned to work at one of the company's other offices which was located in another state. He would work at that location on Monday through Friday but flew home on the weekends. One morning in late December or early January 2005, Applicant visited an adult web-site using his company laptop computer. He downloaded several videos. He agrees that the videos and the web-site were probably X-rated but states they contained no images of sexual intercourse. He admits that he was aware that he was violating company policy when he accessed the adult web-site. He claims that he only viewed the adult web-site using the company laptop computer on that one occasion. After he visited the web-site, numerous pop-ups came up for other adult web-sites. (Tr at 18 – 23)

In late December or early January 2005, Applicant's laptop computer broke down. He contacted the company information technology department and gave them his company laptop in order for them to repair it. While repairing the laptop, a technician discovered pornographic files on Applicant's laptop. This information was forwarded to

Security Operations and Investigations Office on January 7, 2005. (Tr at 23, 43-44: Gov 2; Gov 3)

On January 10, 2005, Applicant was called into the Security Operations and Investigations office. He was interviewed by the manager of the department about the pornography that was found on his company laptop. He initially denied that he accessed the adult web-site using his company laptop. He initially blamed it on his teenage son and his friends. Approximately five to ten minutes into the interview, the investigator asked him how his son was able to access the adult web-site since a password and login was required to access the lap top. Applicant then admitted to accessing the adult web-sites on his lap top but claims that he was using his own separate network. He believed that he had erased the images from the system. (Tr at 24 -29, 49-50)

On February 7, 2005, Applicant was terminated from the company for violation and misuse of information technology. The manager of security operations and investigations testified. He conducted the internal investigation and interviewed Applicant. He personally examined the images on Applicant's company computer and concluded they were pornographic. The computer images were saved and an internal investigation was conducted. He observed approximately 10 to 15 short videos and some still photographs. He observed approximately 1,500 pornographic images on the computer that could not be downloaded. He believes that these pornographic images were viewed and downloaded over a seven-month period on more than one occasion. There were 16 videos and eight pornographic web-sites in the files on Applicant's computer. (Tr at 43-48)

When the manager questioned Applicant he does not recall whether he asked Applicant how many times he may have visited pornographic web-sites. He does not recall Applicant indicating how many times he had accessed pornographic web-sites using the company laptop. (Tr at 50) During the internal company investigation, still pictures and video clips were saved to a DVD. About 1,500 images that were not downloaded on Applicant's laptop were deleted. Applicant's company laptop was then purged of all pornographic images. The laptop was returned to Applicant after the pornographic images were purged. (Tr at 50 -52) The DVD was not presented as part of the government's case.

After Applicant was terminated, he worked as an independent contractor for his current employer. In April 2005, he was hired as a full-time employee. On March 6, 2006, he submitted a Public Trust Position Application, SF 85P. In response to question "7. Your Employment Record," he listed that he was fired from his previous employer on February 7, 2005 for "Violation of company policy regarding personal use of company-provided computer while on TDY." (Gov 1)

Applicant met with an investigator conducting his trustworthiness background investigation on several occasions. (Applicant recalls meeting with the investigator on three occasions. The investigator recalls meeting with Applicant on two occasions. The number of occasions is not relevant to the facts of this case.) The investigator first met with Applicant on October 24, 2007, to discuss Applicant's termination from his previous

employer for misusing the computer. He authenticated the summary of the unsworn declaration which he prepared the same day of the interview which is Government Exhibit 3. He does not recall the specific questions asked during the interview. The investigator does not recall discussing the issue pertaining to Applicant initially denying that he was responsible for the pornographic material on the company laptop. (Tr at 63)

In May 2008, the investigator was contacted and asked to have Applicant prepare a written affidavit. He met with Applicant on May 15, 2008, in the parking lot of a fast food chain. Applicant had limited time because he had a conference call that morning. The investigator prepared the affidavit himself with the summary of Applicant's initial interview which is Government Exhibit 3. He wrote the affidavit in the first person. When he met with Applicant, he had Applicant review the affidavit and allowed him the opportunity to make any changes. He had Applicant initial and sign the affidavit. The investigator did not ask Applicant any questions during this meeting. He did not swear Applicant to an oath when he signed the affidavit. (Tr at 61-63, 111-114)

Applicant disputes that he accessed pornography using his company computer numerous times over a seven month period. He claims he visited an adult web-site only once. He claims that when the security office returned the company laptop to him, the pornographic web-sites remained on the computer. He offered AE A and AE B which allegedly contain the links, addresses, and/or the pornographic web-sites that were contained on his company laptop. Both documents are given less weight because Applicant had the opportunity to show these documents to the manager of the Security Operations and Investigations Office to verify that these were the documents they retrieved from his computer during his testimony. He offered these documents after the witness had left since neither side wished to hold him subject to recall after testifying. Applicant said that if there was only one thing that he would take back was that he wished he would have told the truth from the beginning. (Tr at 94 – 107)

Applicant's current supervisor testified that he has known Applicant since 2004. They worked on a contract proposal together when Applicant was employed with his previous company. In 2005, Applicant started work as an independent consultant for the company. He was eventually hired as a full-time employee. The witness supervised Applicant since that time. He still has daily contact with Applicant. He states Applicant's performance reviews state that he meets or exceeds expectations. Applicant's work is exemplary. He is very detail oriented and has a strong work ethic. Applicant is conscientious about time-keeping and billing the proper hours. He has no difficulty following corporate security policies. Applicant passed a reliability check with the Department of Homeland Security. Since working for the company, Applicant has not had any violations pertaining to the misuse of computers. The supervisor states Applicant is very trustworthy and recommends him for a security clearance. (It is noted that Applicant is applying for a position of public trust.) (Tr at 74-83)

A co-worker of Applicant testified that he has known him for over 25 years. Applicant is currently his program manager but they worked together at a prior defense contractor. Their current interaction at work is between every few days to once a week. They occasionally socialize outside of work such as going to lunch or dinner. They

played golf a couple times. He describes Applicant as one of the most honest and "by the rules" people he knows. Applicant follows company policies. He recommends Applicant for a security clearance. The co-worker has a bachelor's degree in computer science. He testified cookies or files can be stored on a computer through a third party without the owner of the computer's knowledge. (Tr at 83 – 90)

Policies

Positions designated as ADP I and ADP II are classified as "sensitive positions." (See Regulation ¶¶ C3.1.2.1.1.7 and C3.1.2.1.2.3.) "The standard that must be met for assignment to sensitive duties is that, based on all available information, the person's loyalty, reliability, and trustworthiness are such that . . . assigning the person to sensitive duties is clearly consistent with the interests of national security." (See Regulation ¶ C6.1.1.1.) The Deputy Under Secretary of Defense (Counterintelligence and Security) Memorandum, dated November 19, 2004, indicates trustworthiness adjudications will apply to cases forwarded to DOHA by the Defense Security Service and Office of Personnel Management. Department of Defense contractor personnel are afforded the right to the procedures contained in the Directive before any final unfavorable access determination may be made. (See Regulation ¶ C8.2.1.)

When evaluating an Applicant's suitability for a public trust position, the Administrative Judge must consider the disqualifying and mitigating conditions in the AG. These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, these guidelines are applied in conjunction with the factors listed in the adjudicative process. The Administrative Judge's over-arching adjudicative goal is a fair, impartial and common sense decision. According to AG ¶ 2(c), the entire process is a conscientious scrutiny of a number of variables known as the "whole person concept." The Administrative Judge must consider all available, reliable information about the person, past and present, favorable and unfavorable, in making a decision.

The protection of the national security is the paramount consideration. AG ¶ 2(b) requires that "[a]ny doubt concerning personnel being considered for access to [sensitive] information will be resolved in favor of national security." In reaching this decision, I have drawn only those conclusions that are reasonable, logical and based on the evidence contained in the record. Likewise, I have avoided drawing inferences grounded on mere speculation or conjecture.

Under Directive ¶ E3.1.14, the Government must present evidence to establish controverted facts alleged in the SOR. Under Directive ¶ E3.1.15, the Applicant is responsible for presenting "witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by applicant or proven by Department Counsel. . . ." The Applicant has the ultimate burden of persuasion as to obtaining a favorable trustworthiness decision.

A person who seeks access to sensitive information enters into a fiduciary relationship with the Government predicated upon trust and confidence. This

relationship transcends normal duty hours and endures throughout off-duty hours. The Government reposes a high degree of trust and confidence in individuals to whom it grants access to sensitive information. Decisions include, by necessity, consideration of the possible risk the Applicant may deliberately or inadvertently fail to protect or safeguard sensitive information. Such decisions entail a certain degree of legally permissible extrapolation as to potential, rather than actual, risk of compromise of sensitive information.

Section 7 of Executive Order (EO) 10865 provides that decisions shall be "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." See also EO 12968, Section 3.1(b) (listing multiple prerequisites for access to classified or sensitive information).

Analysis

USE OF INFORMATION TECHNOLOGY SYSTEMS

The trustworthiness concern relating to the guideline for Use of Information Technology Systems is set out in AG ¶ 39:

> 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 data used for the communication, transmission, processing, manipulation, storage, or protection of information.

The following disqualifying conditions under Guideline M (M DC) apply to Applicant's case:

M DC ¶ 40(e) (unauthorized use of a government or other information technology system)

M DC ¶ 40(f) (introduction, removal, or duplication of hardware, firmware, software, or media to or from any information technology system without authorization, when prohibited by rules, procedures, guidelines or regulations)

Applicant demonstrated extremely poor judgment when he accessed pornographic web-sites using his company laptop. He admits to being aware of the company rules prohibiting the use of company computers to access pornographic web-sites when he accessed the pornographic web-sites suing his company laptop. He had no special authorization for accessing pornographic web-sites using the company computer. Nor did he have permission to download pornographic files on his company

laptop. While there is a dispute as to the extent of pornographic files that Applicant viewed and over what period of time, there is no factual dispute that Applicant violated company policy by accessing pornographic web-sites using his company laptop. As a result, he was terminated after working 24 years for the company.

The concerns under Guideline M can be mitigated. I find that Guideline M Mitigating Condition (M MC) ¶ 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 case doubt on the individual's reliability, trustworthiness, or good judgment) applies to Applicant's case. Although Applicant exercised extremely poor judgment when he accessed the pornography using his company laptop, more than four years has passed since his termination in February 2005. He has been employed full-time with another defense contractor. He has not been involved in similar incidents at his new employer. His current supervisor thinks highly of him and recommends him for a trustworthiness position. His poor judgment in his previous job resulted in the loss of a 24-year career. He clearly learned a lesson. Considering the price Applicant paid for his extreme lapse of judgment, and that more than four years have passed with no similar conduct his current workplace, the concerns raised under Guideline M have been mitigated.

Personal Conduct

The security concern relating to the guideline for Personal Conduct is set out in AG ¶15:

> 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.

There are specific disqualifying conditions which may be raised. With respect to SOR ¶ 2.a which alleges that Applicant denied knowledge of pornographic material on his company laptop when he was interviewed during the internal company investigation in January 2005, the following Personal Conduct Disqualifying Conditions (PC DC) apply to the facts of this case:

PC DC ¶ 16(b) (deliberately providing false or misleading information concerning relevant facts to an employer, investigator, security official, competent medical authority, or other official government representative)

PC DC ¶ 16(e) (personal conduct, or concealment of information about one's conduct, that creates a vulnerability to exploitation, manipulation, or duress, such as (1) engaging in activities which, if known, may affect the person's personal, professional, or

community standing, or (2) while in another country, engaging, in any activity that is illegal in that country or that is legal in that country but illegal in the United States and may serve as a basis for exploitation or pressure by the foreign security or intelligence service or other group)

Applicant admits that he initially lied to the security manager who interviewed him regarding the discovery of pornography on his company laptop. He deliberately provided misleading information by claiming that his son and his son's friends used his company laptop to access his computer. He did so out of concern as to the consequences if he admitted to it.

The personal conduct concern can be mitigated. With respect to SOR ¶ 2.a, I find the following personal conduct mitigating conditions (PC MC) apply:

PC MC ¶ 17(c) (the offense is so minor, or so much time has passed, or the behavior is so infrequent, or it happened under such unique circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment)

PC MC ¶ 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)

PC MC ¶ 17(e) (the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress)

Applicant misled the investigator for approximately ten minutes prior to acknowledging that he actually accessed pornographic web-sites using his company laptop. While his initial denial demonstrated poor judgment, he made the decision to be truthful during the same interview and misled the investigator for only a brief period of time. He acknowledged his behavior. Since that time, he provided full disclosure for the basis for his termination when he submitted his public trust application in March 2006. He has had a successful career for over four years with his current employer, always meeting or exceeding the standards expected of him. No similar incidents have occurred since his termination in February 2005. Applicant mitigated the personal conduct concerns raised under SOR ¶ 2.a.

SOR ¶ 2.b alleges Applicant provided a misleading statement in his written statement provided on May 15, 2008, by not indicating that he first denied that the pornographic material was his when confronted by the security representative about the pornographic content on his government laptop. I find for Applicant with regard to this allegation. The investigator who interviewed Applicant and prepared the statement in question does not recall whether the issue about Applicant's initial denials ever came up during the first interview in October 24, 2007, and on May 15, 2008. The affidavit was

prepared by the investigator for Applicant to sign based on the investigator's summary of October 24, 2007 interview. The investigator did not interview Applicant on May 15, 2008. He met Applicant on that date for Applicant to review and sign the affidavit. He did not ask Applicant to provide him step-by-step details as to what occurred when he was interviewed by the company security investigator during the internal investigation related to the pornography found on Applicant's company laptop. I cannot conclude that Applicant provided misleading information in his May 15, 2008 statement. Given the general questions that were asked, it does not appear Applicant deliberately omitted the fact that he initially denied that he was responsible for the pornography found on his company laptop when he was first confronted. SOR ¶ 2.b is found for Applicant.

Applicant mitigated the concerns raised under Guideline E. The personal conduct concern is found for Applicant.

Whole Person Concept

Under the whole person concept, the Administrative Judge must evaluate an Applicant's eligibility for a security clearance and/or trustworthiness position by considering the totality of the Applicant's conduct and all the circumstances. The Administrative Judge should consider the nine adjudicative process factors listed at AG ¶ 2(a): "(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 individual's age and maturity at the time of the conduct; (5) extent to which participation is voluntary; (6) the presence or absence of rehabilitation and other permanent behavioral changes; (7) the motivation for the conduct; (8) the potential for pressure, coercion, exploitation, or duress; and (9) the likelihood of continuation or recurrence." Under AG ¶ 2(c), the ultimate determination of whether to grant eligibility for a security clearance and/or trustworthiness position must be an overall common sense judgment based upon careful consideration of the guidelines and the whole person concept.

I considered the potentially disqualifying and mitigating conditions in light of all the facts and circumstances surrounding this case. I considered Applicant's 24-year history with his previous employer. I considered that he was a mature adult who was aware of company rules pertaining to accessing pornography using his company laptop. I considered that he initially denied responsibility when he was interviewed by company security personnel regarding the pornography found on his computer. Applicant demonstrated extremely poor judgment which ultimately led to his termination from a company he worked at for over 24 years. However, since then he has successfully worked for another company for over four years with no repeats of similar incidents. He is a valued employee at his current job. Given the severity of the consequences resulting from Applicant's poor judgment, it is unlikely that he will repeat similar conduct in the future. Applicant learned a very difficult lesson. He mitigated the security concerns raised under Guideline M and Guideline E and demonstrated that he is worthy to be granted a position of public trust.

Formal Findings

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

Paragraph 1 Guideline M:	FOR APPLICANT
Subparagraph 1.a:	For Applicant
Paragraph 2 Guideline E:	FOR APPLICANT
Subparagraph 2.a:	For Applicant
Subparagraph 2.b:	For Applicant

Conclusion

In light of all of the circumstances presented by the record in this case, it is clearly consistent with national security to grant Applicant eligibility for a trustworthiness position. Eligibility for a position of public trust is granted.

_____
ERIN C. HOGAN
Administrative Judge