KEYWORD: Personal Conduct; Criminal Conduct

DIGEST: Applicant is a 28-year-old employee of a defense contractor. He violated rules and regulations by accessing adult web sites on a government computer. Applicant intentionally provided false information in a statement to a government investigator when he denied that he had accessed the adult web sites. Clearance is denied.

CASENO: 05-00381.h1

DATE: 04/20/2007

DATE: April 20, 2007

In re:	)	
	)	
----------	)	ISCR Case No. 05-00381
SSN: ----------	)	
	)	
Applicant for Security Clearance	)	

DECISION OF ADMINISTRATIVE JUDGE
EDWARD W. LOUGHRAN

APPEARANCES

FOR GOVERNMENT
James F. Duffy, Esq., Department Counsel

FOR APPLICANT
Mark S. Zaid, Esq.

SYNOPSIS

Applicant is a 28-year-old employee of a defense contractor. He violated rules and regulations by accessing adult web sites on a government computer. Applicant intentionally provided

false information in a statement to a government investigator when he denied that he had accessed the adult web sites. 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 October 7, 2005, DOHA issued a Statement of Reasons[1] (SOR) detailing the basis for its decision–security concerns raised under Guideline E (Personal Conduct) and Guideline J (Criminal Conduct) of the Directive. Applicant answered the SOR in writing on November 4, 2005, and elected to have a hearing before an administrative judge. The case was assigned to me on December 15, 2006. A notice of hearing was issued on March 6, 2007, scheduling the hearing for March 21, 2007. Applicant waived the 15-day notice requirement. With the consent of the parties, the hearing was conducted as scheduled to consider whether it is clearly consistent with the national interest to grant or continue a security clearance for Applicant. The Government offered six exhibits that were marked as Government Exhibits (GE) 1 through 6, and admitted without objection. Department Counsel's list of exhibits was marked as Hearing Exhibit (HE) II. Applicant testified and offered four exhibits that were marked Applicant Exhibits (AE) A through D, and admitted without objection. DOHA received the hearing transcript (Tr.) on March 30, 2007.

RULINGS ON PROCEDURE

Department Counsel requested that three witnesses testify via video teleconference (VTC). Applicant did not object, and the three Government witnesses testified via VTC. E-mail correspondence on this subject was marked as HE I.

Department Counsel requested that administrative notice be taken of provisions of the Joint Ethics Regulation (HE III), the calendar for 2001 (HE IV), and 18 U.S.C. § 1001 (HE V). Applicant did not object, and I took administrative notice of those items.[2]

FINDINGS OF FACT

Applicant's admissions to the allegations in the SOR are incorporated herein. In addition, after a thorough and careful review of the pleadings, exhibits, and testimony, I make the following findings of fact.

Applicant is a 28-year-old employee of a defense contractor. He is a high school graduate. Applicant enlisted in the U.S. Army right out of high school. He served four years, and was honorably discharged as a Sergeant (E-5). He has held a security clearance since he was in the Army. Applicant is single with no children.[3]

---

[1]Pursuant to Exec. Or. 10865, *Safeguarding Classified Information within Industry* (Feb. 20, 1960), as amended, and Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (Jan. 2, 1992), as amended (Directive).

[2]Tr. at 15-17.

[3]Tr. at 112-114, 146; GE 1.

After he left the Army, Applicant obtained a temporary job through a staffing agency. Applicant was employed by the staffing agency, but worked directly for a defense contractor in a Sensitive Compartmented Information Facility (SCIF), aboard a military installation. Applicant's supervisors were employees of the defense contractor company, not the staffing agency. He was hired to temporarily fill a position until a full time employee could be hired. His employment dates were set to run from June 2001 through September 15, 2001.[4]

Applicant did not have SCI access at that time and had to be escorted while he was in the SCIF. Applicant used his government computer to access adult web sites on several occasions. The web sites contained images of nude adult women, what is commonly referred to as pornography. When the web sites are accessed, some of the material on the site is automatically saved to the hard drive. The use of the government computer to view pornography was against the Joint Ethics Regulation (JER) and local regulations. Applicant may not have specifically known of the provisions of the JER, but he was aware that accessing pornographic web sites on his government computer was unauthorized.[5]

There is conflicting evidence as to whether Applicant was assigned a password and was able to log onto the system by himself, or if he had to be logged on by someone else. Applicant testified that he never received a password, and would be logged onto the system by another employee. The government witnesses testified they believed that Applicant was issued his own password and access, but acknowledged that they were uncertain of that fact.[6] I find that there is insufficient evidence to prove that Applicant had his own password, and was able to log onto the system on his own.

Prior to Applicant's projected employment end date of September 15, 2001, the defense contracting company hired a full time employee for Applicant's position. The area supervisor informed Applicant that they hired a full time employee, and that Applicant's last day of work would be Friday, September 7, 2001.[7]

Monday, September 3, 2001, was Labor Day. Applicant received a paid day off for this holiday. Applicant's area supervisor was off work on Tuesday, September 4, 2001.[8]

Security personnel at the military installation monitored the computer system for unauthorized use. The security personnel identified that a computer in Applicant's area was accessing adult web sites. In the afternoon of September 4, 2001, security personnel monitored Applicant's computer and saw that it was accessing an adult web site. They went to the SCIF and checked the computers in the room. Applicant had viewed adult web sites within fifteen minutes of the arrival of the security personnel. Security stopped at Applicant's computer and verified it was the computer in question. Applicant was sitting at the computer when the security personnel arrived

[4]Tr. at 52-58, 116-117; Applicant's response to SOR; GE 3, 4, 6; AE A.

[5]Tr. at 21-22, 120-121; Applicant's response to SOR; HE III.

[6]Tr. at 31, 55-56, 60-61, 73-74; Applicant's response to SOR.

[7]Tr. at 56-58.

[8]Tr. at 58; HE IV.

to check his computer. He was asked to leave the SCIF, and was escorted out of the SCIF by the acting area supervisor. Security personnel verified that Applicant's computer was the one that visited adult web sites, and they seized the computer. Security personnel informed Applicant's supervisor when he returned to the SCIF that they found pornography on the computer. The supervisor left the room and told Applicant that they found pornography on the computer. Applicant was then sent home. Applicant's time card shows he ended work one and a half hours early.[9]

The staffing agency called Applicant that evening and told him that he was no longer needed at the work site and that his contract was done. The company made no mention of his accessing pornography, and did not tell him he was terminated.[10] When asked at the hearing what his understanding at that time was as to when his last day of work would be, Applicant stated that he thought his last day of work would be "some time within that next week and a half,"[11] and that:

> I knew that it had been shortened or originally it was extended because the person quit. They needed to find somebody else to replace that position. I didn't know how long or how short it was going to be. When I received that phone call I just assumed that they had found somebody and they no longer were going to need me there.[12]

Applicant was interviewed by an investigator for the Defense Security Service (DSS) on November 21, 2002, and provided a written statement. Applicant was questioned about the events that occurred during his last day of employment in September 2001. Applicant denied accessing pornographic web sites. This was a knowing and willful false statement. He stated that he was never "accused of violating or misusing information technology."[13] I also find this was a knowing and willful false statement.

Applicant wrote in the statement that each time he worked on the computer that another employee had to log him onto the computer.[14] There is insufficient evidence to make a determination that this was a false statement.

Applicant further stated that September 5, 2001, was to be his, "last day of employment due to end of contract," and that it was "coincidental the last day of the contract happened to be the day that they confiscated the computer."[15] I find that this was a knowing and willful false statement by Applicant.

---

[9]Tr. at 23-29, 42-43, 71-79; GE 4; GE 5 at 2; AE A.

[10]Tr. at 122-123; Applicant's response to SOR.

[11]Tr. at 148.

[12]*Id.* at 123-124.

[13]GE 2.

[14]*Id.*

[15]*Id.* The statement incorrectly notes throughout that September 5, 2001, and not the correct date of September 4, 2001, was the date of the incident.

Applicant responded to the SOR on November 4, 2005. He admitted that he accessed pornography on his government computer, and stated, "[t]his was a one time transgression that I very much regret." Applicant admitted he lied in his statement when he wrote that he "never accessed a pornographic web site," but denied that he lied in other parts of the statement. Applicant wrote in his response:

> On my last day of employment, my actual supervisor was not at work. Therefore, I was being escorted by another employee that worked in the same area as I did. After lunch he had to go to a meeting and since I was not permitted to be in the area by myself he told me to go home for the day. I simply casually left the building as I did on any other day. Once I got home I received a phone call from [staffing company] saying that they no longer needed me for that job, but no reason was given as to why. It was my understanding at the time that September 5, 2001, was to be my last day of work. That is why when I was told by [staffing company] on September 4, 2001, that I was not needed to stay I understandably did not think anything of it.[16]

Applicant testified that he was never told that he was suspected or accused of accessing pornography on the computer.[17] Since I found that Applicant was told that September 7, 2001 was to be his last day of work, and that he was informed that pornography was found on his computer, I find that Applicant intentionally provided false information in his response to the SOR, and during his testimony at his hearing.

Applicant is highly regarded by those who know him from the Army and from working with him. He is described as a man of strong values and integrity, honest, candid, someone who has always been one for upholding high standards, adheres to regulations, and is a strong advocate of network security. His character letters confirm that they are aware of the allegations against Applicant. They believe it to be an isolated incident, and that Applicant has learned his lesson.[18] His character witnesses testified similarly.

POLICIES

"[N]o one has a 'right' to a security clearance."[19] 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

---

[16]Applicant's response to the SOR.

[17]Tr. at 122. Any false information provided by Applicant in his response to the SOR or at the hearing is not considered for disqualifying purposes, but may be considered in assessing Applicant's credibility, when analyzing the "whole person," and the potential application of mitigating conditions.

[18]AE B-D.

[19]*Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988).

access to such information."[20] The President authorized the Secretary of Defense or his designee to grant applicants eligibility for access to classified information "only upon a finding that it is clearly consistent with the national interest to do so."[21] An applicant has the ultimate burden of demonstrating that it is clearly consistent with the national interest to grant or continue his or her security clearance. The clearly consistent standard indicates that security clearance determinations should err, if they must, on the side of denials.[22] Any reasonable doubt about whether an applicant should be allowed access to sensitive information must be resolved in favor of protecting such sensitive information.[23] The decision to deny an individual a security clearance is not necessarily a determination as to the loyalty of an applicant. 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.[24]

The Directive sets forth potentially disqualifying conditions (DC) and mitigating conditions (MC) under each guideline. Additionally, each security clearance decision must be a fair and impartial commonsense decision based on the relevant and material facts and circumstances, the whole-person concept, along with the adjudicative process factors listed in ¶ 6.3 and ¶ E2.2.1 of the Directive.

Conditions that could raise a security concern and may be disqualifying, as well as those which would mitigate security concerns, pertaining to the adjudicative guidelines are set forth and discussed in the conclusions section below.

CONCLUSIONS

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

Guideline E, Personal Conduct

Conduct involving questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations could indicate that the person may not properly safeguard classified information.

Personal Conduct Disqualifying Condition (PC DC) E2.A5.1.2.1 (*Reliable, unfavorable information provided by associates, employers, coworkers, neighbors, and other acquaintances*),

---

[20] *Id.* at 527.

[21] Exec. Or. 10865, *Safeguarding Classified Information within Industry* § 2 (Feb. 20, 1960).

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

[23] *Id.*; Directive, ¶ E2.2.2.

[24] Exec. Or. 10865 § 7.

and PC DC E2.A5.1.2.4 (*Personal conduct or concealment of information that increases an individual's vulnerability to coercion, exploitation, or duress, such as engaging in activities which, if known, may affect the person's personal, professional, or community standing or render the person susceptible to blackmail*) apply to Applicant's accessing pornography on his government computer.

PC DC E2.A5.1.2.3 (*Deliberately providing false or misleading information concerning relevant and material matters to an investigator, security official, competent medical authority, or other official representative in connection with a personnel security or trustworthiness determination*), and PC DC E2.A5.1.2.4 apply to Applicant's intentional false statement to the investigator.

Applicant admitted he lied in one part of his statement, but he denied lying in other parts. I observed Applicant during his testimony, and assessed his demeanor and credibility. I considered all the evidence, including Applicant's inconsistent statements, and admission that he lied to the investigator about one aspect of the incident. I considered that the government witness testified that he could not state that he was "absolutely sure" that he mentioned to Applicant that pornography was found on the computer.[25] I weighed the witness' testimony with Applicant's denials. I also considered Applicant's version of events that the acting supervisor told him that he had to go to a meeting, and that since Applicant needed an escort, Applicant should go home, so Applicant "simply casually left the building as [he] did on any other day."[26] The witness never testified about a meeting. Applicant's version of events is not credible.

After considering all the evidence, I find that Applicant deliberately provided false information to the DSS investigator when he denied accessing pornographic web sites, when he stated that he was never accused of violating or misusing information technology, and when he stated that the day of the incident was to be the last day of his contract.

I do not find that Applicant was "terminated" from his employment. Applicant was not employed by the contractors at the military installation. They could not terminate his employment. He was employed by the staffing agency. I am satisfied that the staffing agency simply told Applicant that he was no longer needed at the installation. While I find that Applicant provided more than one false fact in his statement, as substantially alleged in SOR ¶¶ 1.b and 1d, there was only one statement.[27] I find this amounts to a single incident of falsification.

In his statement, Applicant wrote that he had to be logged onto the computer by another employee. There is insufficient evidence for a finding that the statement was false in that regard. I conclude SOR ¶ 1.c in Applicant's favor.

---

[25]Tr. at 78.

[26]Applicant's response to SOR at 2.

[27]Part of the allegations in SOR ¶¶ 1.b and 1.d, were that Applicant was terminated from employment, and that the end of his contract was September 15, 2001. I do not find those specific facts.

I considered all the mitigating conditions and specifically considered Personal Conduct Mitigating Condition (PC MC) E2.A5.1.3.2 (*The falsification was an isolated incident, was not recent, and the individual has subsequently provided correct information voluntarily*), PC MC E2.A5.1.3.3 (*The individual made prompt, good-faith efforts to correct the falsification before being confronted with the facts*), PC MC E2.A5.1.3.4 (*Omission of material facts were caused or significantly contributed to by improper or inadequate advice of authorized personnel, and the previously omitted information was promptly and fully provided*), and PC MC E2.A5.1.3.5 (*The individual has taken positive steps to significantly reduce or eliminate vulnerability to coercion, exploitation, or duress*).

Applicant was not completely honest to the DSS investigator and at the hearing about what occurred when he was viewing pornography on the government computer. He has not significantly reduced his vulnerability to coercion, exploitation, or duress. Without complete candor, I cannot apply PC MC E2.A5.1.3.5.

The Appeal Board has established the difference between PC MC E2.A5.1.3.2 and PC MC E2.A5.1.3.3 when analyzing their application in a falsification case:

> Mitigating Condition 2 [E2.A5.1.3.2] is properly used in a case where the falsification is old and the applicant subsequently provides correct information to the government about other matters not covered by the old falsification (to elaborate, in a hypothetical case, if an applicant made a false declaration in 1986 but subsequently provided truthful statements about matters other than the false declaration in his re-investigations in 1992 and 1999 and did not repeat the false declaration, then Mitigating Condition 2 would be applicable). In a situation where an applicant seeks to correct a falsification, such as the instant case, the potentially applicable factor, if there is one, is Mitigating Condition 3 [E2.A5.1.3.3], not Mitigating Condition 2.[28]

Application of PC MC E2.A5.1.3.3 in Applicant's favor requires that Applicant meet his burden of establishing that he made prompt, good-faith efforts to correct his false statement to the DSS investigator before being confronted with the facts.[29] His partial admissions in response to the SOR and at the hearing do not constitute a prompt, good-faith effort to correct his falsification before being confronted with the facts. No mitigating condition is applicable.

Guideline J, Criminal Conduct

A history or pattern of criminal activity creates doubt about an applicant's judgment, reliability, and trustworthiness.

It is a criminal offense to knowingly and willfully make any materially false, fictitious, or fraudulent statement or representation in any matter within the executive branch of the Government of the United States. 18 U.S.C. § 1001. Security clearances are within the jurisdiction of the

[28]ISCR Case No. 99-0557 (App. Bd. Jul. 10, 2000).

[29]*See, e.g.,* ISCR Case No. 02-10502 (App. Bd. April 29, 2004).

executive branch of the Government of the United States.[30] A violation of 18 U.S.C. § 1001 is a serious offense as it may be punished by imprisonment for up to five years. Applicant knowingly and willfully made a materially false statement to an authorized investigator, as discussed above. Criminal Conduct Disqualifying Condition (CC DC) E2.A10.1.2.1 (*Allegations or admissions of criminal conduct, regardless of whether the person was formally charged*), and CC DC E2.A10.1.2.2 (*A single serious crime or multiple lesser offenses*) both apply.

I have considered all the mitigating conditions and especially considered Criminal Conduct Mitigating Condition (CC MC) E2.A10.1.3.1 (*The criminal behavior was not recent*), CC MC E2.A10.1.3.2 (*The crime was an isolated incident*), and CC MC E2.A10.1.3.6 (*There is clear evidence of successful rehabilitation*), and conclude none apply. Applicant knowingly and willfully made a false statement. I further find that he intentionally submitted false information in his response to the SOR, and provided false testimony at his hearing. Under those circumstances, no mitigating condition applies.

Whole Person Analysis

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. Available, reliable information about the person, past and present, favorable and unfavorable, should be considered in reaching a determination. In evaluating Applicant's case, I have considered the adjudicative process factors listed in the Directive. I have also considered every finding of fact and conclusion discussed above.

I considered Applicant's military record and Honorable Discharge. I also considered Applicant's age and favorable character evidence. That evidence is insufficient to overcome the poor judgment, untrustworthiness, dishonesty, and unwillingness to comply with rules and regulations which Applicant displayed by accessing pornography on a government computer, and then lying about it.

After weighing the disqualifying and mitigating conditions and evaluating all the evidence in the context of the whole person, I conclude Applicant has not mitigated the security concerns based on his personal conduct and criminal conduct.

FORMAL FINDINGS

The following are my conclusions as to each allegation in the SOR:

Paragraph 1. Guideline E:	AGAINST APPLICANT
Subparagraph 1.a:	Against Applicant
Subparagraph 1.b:	Against Applicant
Subparagraph 1.c:	For Applicant
Subparagraph 1.d:	Against Applicant

[30] *See Egan*, 484 U.S. at 527.

Paragraph 2. Guideline J: 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.

Edward W. Loughran
Administrative Judge