DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 06-02841
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Ray T. Blank, Jr., Esq., Department Counsel
For Applicant: *Pro Se*

July 10, 2008

Decision

LOUGHRAN, Edward W., Administrative Judge:

Applicant did not mitigate the Personal Conduct and Use of Information Technology Systems security concerns. Eligibility for access to classified information is denied.

On February 12, 2008, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) to Applicant detailing the security concerns under Guideline E, Personal Conduct and Guideline M, Use of Information Technology Systems. 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.

Applicant answered the SOR on March 13, 2008, and requested a hearing before an Administrative Judge. The case was assigned to me on May 6, 2008. DOHA issued

a notice of hearing on May 12, 2008, and the hearing was convened as scheduled on June 17, 2008. DOHA received the transcript of the hearing (Tr.) on June 24, 2008.

Evidentiary Rulings

The Government offered Exhibits (GE) 1 through 8. GE 1, 2, and 4 through 8 were received without objection. Applicant originally objected to GE 3, a report of investigation (ROI) of an interview. The objection was sustained. Applicant later withdrew his objection and GE 3 was admitted. Applicant testified on his own behalf, and offered Exhibits (AE) A through J, which were received without objection.

Findings of Fact

Applicant is a 38-year-old employee of a defense contractor. He has been with his current employer since 2002. He obtained a bachelor's degree in 2005. He is married with two children, ages 12 and 10.[1]

Applicant was a systems administrator for a company (company A) from about 1998 to 2000. Part of his responsibilities included monitoring the employees' e-mail traffic for viruses and unauthorized or illegal usage. Employees were informed that their e-mails were subject to monitoring. Applicant periodically read more of the e-mails than was necessary to accomplish his job of monitoring the system.[2]

Applicant worked for another company (company B) from about 2000 to 2002. He was in charge of the Information Technology (IT) department of the company. Applicant was again responsible for monitoring the company's e-mail and internet traffic. Applicant again read more of the employees' e-mails than his job required. While working at companies A and B, Applicant installed company software on his home computer without the proper authorization.[3]

Applicant started working for his current employer (company C) in 2002. He does not have the same responsibilities of monitoring the company's e-mail and internet traffic that he held at the previous companies. On at least one occasion, he accessed and read his supervisor's e-mail without permission or authorization. Applicant testified that he has since told the supervisor what he did and the supervisor was "comfortable with it." Applicant introduced a character letter from this supervisor. The incident is not mentioned in the letter. Applicant has never been reprimanded or otherwise disciplined for any of his actions at the three companies.[4]

[1] Tr. at 58-59, 63-64; GE 1.

[2] Tr. at 33-35, 56-57, 68-79; GE 1, 3.

[3] Tr. at 35-38, 40-44, 79-81, 81-87; Applicant's response to SOR; GE 1, 3.

[4] Tr. at 38-40, 62, 70, 81-82, 114-115; Applicant's response to SOR; GE 1, 3; AE C.

Applicant provided differing accounts of the above events. He provided a written statement to a background investigator on May 7, 2003. He discussed his employment at company A:

> At no such time at [company A] or since then have I illegally accessed data or not complied with computer or company security policies. I have not used any information that may have been available to me in the course of my position and network security rights for any personal gain, or malicious intent.[5]

Applicant denied that he intentionally misled the investigator by failing to discuss the incidents with his employers. He testified that he does not feel he ever illegally accessed data or e-mail as his job required him to monitor the e-mails.[6]

Applicant also discussed his marijuana use in the 2003 statement. He admitted to using marijuana on three occasions in 2001 and 2002. He wrote that his use in 2001 was the first time he used marijuana. He also wrote that he had "not used any other drugs." In a later statement, he admitted that he used marijuana and other illegal drugs as early as 1991.[7]

Applicant was interviewed on October 14, 2004, in conjunction with a polygraph, for a determination by another government agency of Applicant's eligibility for access to Sensitive Compartmented Information (SCI). A written statement was not taken, but the interviewer summarized the interview in a report of investigation (ROI).[8] There was no evidence introduced about how and when the report was prepared. Applicant admitted that he misused his responsibilities at company A and crossed the line out of curiosity once or twice a day for a month or two near the end of his term of employment. He admitted to looking at his supervisor's e-mail to see what she thought of him. He also admitted to looking for general office gossip. The report further noted:

> When confronted with the above information from the background investigator, SUBJECT stated HE was not honest. HE was surprised when confronted with the information. HE did not tell them because HE was embarrassed and surprised.[9]

---

[5] GE 7.

[6] Tr. at 44-48; Applicant's response to SOR.

[7] GE 7, 8. Applicant's drug use was not alleged in the SOR and is not considered for disqualifying purposes. It was also not alleged that he falsified the 2003 statement regarding his drug use, and that is also not considered for disqualifying purposes. The entire statement is considered when gauging Applicant's credibility, in the application of mitigating conditions, and in the whole person analysis.

[8] Tr. at 40; GE 3. The results of the polygraph were not offered into evidence. The polygraph is only considered for the impact, if any, it had on Applicant's statement.

[9] GE 7. Emphasis in original.

Applicant testified that he was discussing the 2003 statement when he made the above comments to the investigator.[10]

Applicant admitted during the October 14, 2004 interview that while with company B, he looked at his supervisor's e-mail and other employees' e-mail approximately 50 times over two years. He admitted that he read the e-mail of his supervisor at his current employer about five times since he started in 2002. He stated he did it to see what was going on and to keep him up-to-date as his supervisor did not check his e-mail everyday. He admitted that he installed company software on his home computer both with and without permission. He estimated that he installed about ten applications without permission. He also admitted driving while intoxicated approximately once per year over the previous five years.[11] Applicant was denied access to SCI by the other government agency in 2004.[12]

Applicant provided a written statement to a background investigator on August 9, 2007. The investigator had either a copy of the 2004 ROI or the denial of Applicant's SCI, which summarized the ROI, or both, prior to the interview and written statement. Regarding his actions at company A, he wrote his "position at this work was to review e-mails that went through the company's system. I believe I went over the line of reviewing e-mail or reading more of the specifics of e-mails than I was required to do." He discussed his actions at company B, and wrote the company "did not know that I was doing this action at their facility, however, I believed at the time that this was my responsibility for working at this facility. I did not believe I broke any policy for my job title nor responsibilities." Further in the statement he wrote that his "violation was reading more e-mail than [he] was requested to do." It is not perfectly clear which company this statement referred to, but immediately before the sentence he discusses the time period of "2000 to 2002," which coincided with his employment at company B. He also admitted to misusing network security privileges at his current company between September 2002 and approximately March 2003.[13]

Applicant also wrote in the August 2007 statement: "I admit to driving while intoxicated one time over the last five years."[14] I do not find this statement to be inconsistent with Applicant's prior admission in October 2004, that he drove while intoxicated approximately once per year over the previous five years.

[10] Tr. at 87-89.

[11] GE 3, 7. Applicant's driving while intoxicated was not alleged in the SOR and is not considered for disqualifying purposes. It is considered solely for the purpose of deciding whether he provided false information about his drinking and driving in a subsequent statement.

[12] GE 2, 4-6.

[13] Tr. at 90; GE 8.

[14] GE 8.

In Applicant's response to the SOR dated March 13, 2008, he denied the allegations in the SOR that reflected his unauthorized access of e-mails at companies A and B. Regarding company A, he wrote "[a]t no time did I access another person's e-mail without permission. I received permission from my supervisor when she asked me to be in charge of the network and security for [company A]." He provided a similar denial regarding company B, stating his actions were pursuant to his responsibilities. These statements may be technically true. However, they are incomplete and misleading. He admitted to SOR ¶ 1.c, which alleged the access of his supervisor's e-mail at his current employer without permission. He stated it was a one-time incident that occurred more than five years previous and has not been repeated since then. This is inconsistent with Applicant's previous admissions that he read his current supervisor's e-mails on about five occasions.

Applicant testified he was authorized to install the applications on his home computer, as the companies had sufficient licenses from the software companies and he was the one who decided who could have the software placed on their home computers. He initially admitted during testimony that he looked through his current supervisor's e-mail a "handful" of times, which he thought was "less than five." He later testified that he only looked at his supervisor's e-mail without authorization on one occasion, but that he accessed his computer about three or four times.[15]

Character letters on Applicant's behalf describe him as loyal to the United States, professional, honest, ethical, truthful, dedicated, efficient, competent, responsible, and reliable. His performance appraisals are excellent.[16]

Policies

When evaluating an applicant's suitability for a security clearance, the Administrative Judge must consider the revised adjudicative guidelines (AG). In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially disqualifying conditions and mitigating conditions, which are to be used in evaluating an applicant's eligibility for access to classified information.

These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, Administrative Judges apply the guidelines 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.

[15] Tr. at 81-87, 114-115.

[16] AE C-J.

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 classified 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 the applicant or proven by Department Counsel." The applicant has the ultimate burden of persuasion for obtaining a favorable security decision.

A person who seeks access to classified 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 classified information. Decisions include, by necessity, consideration of the possible risk the applicant may deliberately or inadvertently fail to protect or safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation as to potential, rather than actual, risk of compromise of classified information.

Section 7 of Executive Order 10865 provides that adverse 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

Guideline M, Use of Information Technology Systems

The security 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 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.

AG ¶ 40 describes conditions that could raise a security concern and may be disqualifying. The following are potentially applicable:

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

(c) use of any information technology system to gain unauthorized access to another system or to a compartmented area within the same system;

(e) unauthorized use of a government or other information technology system; and

(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 was in charge of monitoring the e-mail and internet for viruses and unauthorized use at his first two companies. Viewing employees' e-mail was part of his job. Once he verified that there was nothing of concern with the e-mails, that should have been the end of it. Instead, he would periodically read employees' e-mails for his own reasons. He did not have the same responsibilities at his current employer, but he again read his supervisor's e-mail without permission or authorization. His actions at the three companies establish AG ¶¶ 40(a), (c), and (e).

Applicant installed company software on his home computer. He has vacillated between stating it was without permission and it was authorized. I find his statement pursuant to a polygraph that it was without permission to be the most credible. AG ¶ 40(f) has also been established.

Conditions that could mitigate the Use of Information Technology Systems security concerns are provided under AG ¶ 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;

(b) the misuse was minor and done only in the interest of organizational efficiency and effectiveness, such as letting another person use one's password or computer when no other timely alternative was readily available; and

(c) the conduct was unintentional or inadvertent and was followed by a prompt, good-faith effort to correct the situation and by notification of supervisor.

It has been a number of years since Applicant committed the IT conduct alleged in the SOR. Because Applicant has not been totally truthful, I am unable to find that the conduct is unlikely to recur and does not cast doubt on his reliability, trustworthiness, or good judgment. AG ¶ 41(a) is not applicable. The actions were intentional and they

were not done in the interest of organizational efficiency and effectiveness. AG ¶¶ 41(b) and (c) have no applicability in this case.

Guideline E, 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.

AG ¶ 16 describes conditions that could raise a security concern and may be disqualifying. The following are potentially applicable:

> (a) deliberate omission, concealment, or falsification of relevant facts from any personnel security questionnaire, personal history statement, or similar form used to conduct investigations, determine employment qualifications, award benefits or status, determine security clearance eligibility or trustworthiness, or award fiduciary responsibilities;
>
> (b) refusal to provide full, frank and truthful answers to lawful questions of investigators, security officials, or other official representatives in connection with a personnel security or trustworthiness determination; and
>
> (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.

Applicant's actions at his current and two prior companies raised Information Technology concerns, as addressed above. Those same actions are sufficient to raise AG ¶ 16(e), as personal conduct that created a vulnerability to exploitation, manipulation, or duress.

Applicant denied intentionally omitting the information about his actions at his last three companies from his May 7, 2003 statement. After considering all the evidence, I find that it was an intentional omission designed to deceive the investigator. AG ¶¶ 16(a) and (b) have been established for SOR ¶ 1.e.

There is insufficient evidence for a finding that Applicant falsified the August 9, 2007 statement, as alleged in SOR ¶ 1.f. While I find the 2007 statement to be somewhat disingenuous, there is also insufficient evidence that he falsified the

statement, as specifically alleged in SOR ¶ 1.g. SOR ¶¶ 1.f and 1.g are concluded for Applicant.

The fact that Applicant was denied access to SCI in 2005, based upon much of the conduct that is addressed in these proceedings does not independently raise any disqualifying condition. SOR ¶ 1.h is concluded for Applicant.

Conditions that could mitigate Personal Conduct security concerns are provided under AG ¶ 17. The following are potentially applicable:

> (a) the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts;
>
> (b) the refusal or failure to cooperate, omission, or concealment was caused or significantly contributed to by improper or inadequate advice of authorized personnel or legal counsel advising or instructing the individual specifically concerning the security clearance process. Upon being made aware of the requirement to cooperate or provide the information, the individual cooperated fully and truthfully;
>
> (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;
>
> (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;
>
> (e) the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress; and
>
> (f) the information was unsubstantiated or from a source of questionable reliability.

Applicant no longer works for two of the companies involved. That significantly reduces his vulnerability to exploitation, manipulation, or duress. AG ¶ 16(e) is applicable for SOR ¶¶ 1.a, 1.b, and 1.d. He still works for the company and supervisor that were involved in part of his personal conduct. While he testified that he told his current supervisor that he read his e-mail, the supervisor's letter does not mention this fact. AG ¶ 16(e) is not applicable for SOR ¶ 1.c. Because Applicant has been less than totally truthful throughout the process, I am unable to find any other mitigating condition.

Whole Person Concept

Under the whole person concept, the Administrative Judge must evaluate an Applicant's eligibility for a security clearance 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) the 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 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. Applicant's IT issues all occurred several years ago. He is highly regarded at his current company and presented very favorable character evidence. However, he presented false, incomplete, and misleading information throughout the process. The most accurate information was obtained while Applicant was under the scrutiny of a polygraph. Without the sword of a polygraph hanging over his head, Applicant cannot be trusted to provide truthful responses.

Overall, the record evidence leaves me with questions and doubts as to Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude Applicant has not mitigated the Personal Conduct and Use of Information Technology Systems security concerns.

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 E:	AGAINST APPLICANT
Subparagraphs 1.a-1.b:	For Applicant
Subparagraph 1.c:	Against Applicant
Subparagraph 1.d:	For Applicant
Subparagraph 1.e:	Against Applicant
Subparagraphs 1.f-1.h:	For Applicant

Paragraph 2, Guideline M:	AGAINST APPLICANT
Subparagraph 1.a:	Against Applicant

Conclusion

In light of all of the circumstances presented by the record in this case, it is not clearly consistent with the interest of national security to grant Applicant eligibility for a security clearance. Eligibility for access to classified information is denied.

_____
Edward W. Loughran
Administrative Judge