DATE: November 30, 2006

In re:

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

Applicant for Security Clearance

ISCR Case No. 03-21688

DECISION OF ADMINISTRATIVE JUDGE

CHRISTOPHER GRAHAM

APPEARANCES

FOR GOVERNMENT

Sabrina Redd, Esq., Department Counsel

FOR APPLICANT

Dennis J. Sysko, Esq.

SYNOPSIS

Applicant is a senior scientist and chief technologist for a defense contractor. From about 1985 to 1996, he downloaded government software to his personal computer so he could work at home. He also made two inadvertent security violations in 2003. Additionally, he conducted correspondence with women in an Eastern Bloc country, and when confronted at work, lied about it, and filed a false incident report with OSI investigators. He did not inform his wife of his misconduct until after he received the Statement of Reasons (SOR). The government failed to make its case under Guideline M (misuse of information technology systems) and he successfully mitigated the security concerns under Guideline K (security violations.) His lack of trustworthiness and good judgment, however, raise security concerns about Guideline E (personal conduct). 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. As required by Department of Defense Directive 5220.6 ¶ E3.1.2 (Jan. 2, 1960), as amended, DOHA issued a Statement of Reasons (SOR) on October 27, 2005, detailing the basis for its decision - security concerns raised under Guideline M (Information Technology), Guideline K (Security Violations), and Guideline E (Personal Conduct) of the Directive. Applicant answered the SOR in writing on November 11, 2005 and elected to have a hearing before an administrative judge. The case was assigned to another administrative judge on March 29, 2006, but because Applicant decided he wanted the hearing at a location closer to his attorney, it was transferred to me on July 19, 2006. Notice of Hearing was issued on September 12, 2006. I convened a hearing on September 21, 2006, to consider whether it is clearly consistent with the national interest to grant or continue a security clearance for Applicant. The government offered five exhibits, marked as exhibits 1-5. Applicant offered six exhibits, marked as exhibits A-F. The government objected to exhibits E and F. The objections were overruled.[(1)] DOHA received the hearing transcript (Tr.) on September 29, 2006.

FINDINGS OF FACT

Applicant admitted all the factual allegations pertaining to misuse of information technology systems under guideline M (subparagraphs 1.a., 1.c., 1.d., 1.e., and 1.f.), all of the factual allegations pertaining to security violations (subparagraph 2.a.), and all of the factual allegations pertaining to personal conduct under guideline E (subparagraphs 3.a. through 3.d.) He denied the allegations contained in subparagraph 1.b. Those admissions are incorporated herein as findings of fact. After a complete and thorough review of the evidence in the record, and upon due consideration of same, I make the following additional findings of fact:

Applicant is a 47-year-old senior scientist and chief technologist for a defense contractor.[(2)] He served in the U.S. Air Force (USAF) from 1978 until 1997.[(3)] He has held a top secret clearance since 1979.[(4)] He enlisted in the USAF as a high school graduate. Because his test scores were so high during his military career, the USAF sent him to school to complete work on bachelor, master, and doctor of philosophy degrees in electrical engineering. He completed officer candidate school, retiring as a major.[(5)] Applicant has been granted five patents, four assigned to the USAF, and one to his current employer.[(6)] He is married and has three children.[(7)]

Misuse of Information Technology Systems

In 1985, Applicant copied a word processing program belonging to a university, to use on his personal computer.[(8)] He used the program to publish on behalf of the university and the USAF. He received no remuneration for his work, and was unaware if there was a university policy with regard to copying software.[(9)] In 1986, he was a research and development officer for the USAF and a student working on his masters. He took a copy of computer software programs from a military weapons laboratory so he could work at home from 6-10 PM, because his wife was complaining about the long hours he was spending at his office. He was unaware of any computer software policy, because he asked for the software and it was given to him. He used the program to conduct research for the USAF and which was published by the USAF.[(10)] In 1990, he copied to his personal computer a word equation writer and other programs belonging to a university. The software custodian gave him the programs. He was unaware of any prohibition against copying the software. He was working on his Ph.D. sponsored by the USAF Academy. The student version of the programs that came with his computer were not sophisticated enough to enable him to do his research.[(11)] In 1995 and 1996, he used a government computer belonging to the USAF to "surf the Internet" after working hours. He was unsure about USAF policy concerning personal use of the internet. He had heard discussions of filters being established to prevent access to certain websites, and that the internet could be accessed on a non-interfering basis.[(12)] The alleged misuse of government computers in 1996 involved use of an "open computer" set apart for the employees to check emails, etc., using an unclassified computer.[(13)] Also in 1996, he scanned a personal photograph of himself onto the USAF "open computer," then e-mailed it to his personal computer. He then forwarded his picture to an Internet agency specializing in dating women from Eastern Bloc countries, although still being married. He also had put in his retirement papers to the USAF and was using the open computer to seek employment.[(14)]

Security Violations

In 2003, Applicant committed two security violations for incorporating sensitive information into reports he created on an unclassified computer. These reports contained very subtle violations and were not caught by his employer's program manager or security officer, who reviewed the reports before sending on to the customer. The customer caught the error. He submitted these reports via unclassified e-mail to other recipients whereby a compromise of classified information occurred. His conduct was in violation of his company's security policies and paragraphs 5 - 100, 5 - 403, and 5 - 500, of DOD 5220-22-M., National Industrial Security Program Operating Manual (NISPOM), January 1995. On January 19, 2004, his employer gave him a letter of reprimand.[(15)] He was given additional training and additional staff and the documents were no longer sent via e-mail but were sent by courier or secure fax.[(16)]

Personal Conduct

In addition to the allegations set forth in the above two paragraphs, Applicant set up a private post office box in order to receive correspondence from women in Eastern Bloc countries. He maintained a regular correspondence with a young female from an Eastern Bloc country beginning in about 1996. He was "flirting with her" until at least mid-1997. He then realized she was serious about looking for a way to enter the United States, and he did not want to jeopardize his relationship with his spouse and family. He received letters from about ten females. He never discussed classified information. He soon thereafter sent postcards terminating any relationship.[(17)] Applicant did not tell his spouse about the forwarding of his photo to an Internet agency, setting up a private post office box, and maintaining exchanges of correspondence with a young female from an Eastern Bloc country, until 2006.[(18)] In 1997, when his private post office box was closed, letters from the Eastern Bloc countries were forwarded to his work address. A secretary opened the letters and gave them to Applicant in the presence of co-workers and said, "Somebody's playing a joke on you."[(19)] Applicant agreed with that statement, then filed a false report with the USAF Office of Special Investigations (OSI), attached the letters, and claimed someone was playing a trick on him, denying knowledge of the letters.[(20)] Shortly thereafter, he made a second false report to OSI, dropping off a second set of letters.[(21)]

In February 2006, Applicant told his daughter, a third-year law student, about his "flirting" activities. She recommended he tell his wife and enter therapy. In arch, he told his wife about his activities.[(22)]

Applicant's psychologist was called to testify. After obtaining his Ph. D. in clinical psychology, he spent nine years' active duty with the U.S. Army Medical Corps. In addition to several hours of interviews with Applicant, the doctor conducted a series of personality tests, the most notable being the Minnesota Multi-Phasic Personality Inventory (MMPI) and the Milan Clinical Multiaxial Inventory.[(23)] He found Applicant had no emotional or psychological disorder.[(24)] Applicant moved the admission of Applicant's Exhibit F. At this time, portions of the exhibit were stricken per government objection.[(25)] The doctor's evaluation states that Applicant presented himself as trustworthy, honest, law-abiding, and worthy of holding a security clearance.[(26)] He also stated that in Asian males [like Applicant], embarrassment and humiliation are some of the worst things that can happen in his life.[(27)]

Applicant's wife testified that during his military career, Applicant worked either as a student or as a USAF employee, and she took care of the family.[(28)] Since learning of his correspondence with foreign women, both have attended marriage counseling. They are communicating better, are dealing with their issues, and their marriage is improving.[(29)] He does not discuss his work with her. She considers him to be a loyal and trustworthy person.[(30)]

POLICIES

"No one has a 'right' to a security clearance."[(31)] 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 access to such information."[(32)] 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."[(33)] Each security clearance decision "must be a fair and impartial common sense determination based upon consideration of all the relevant and material information and the pertinent criteria and adjudication policy."[(34)]

An applicant "has the ultimate burden of demonstrating that it is clearly consistent with the national interest to grant or continue his security clearance."[(35)]

Enclosure 2 of the Directive sets forth personnel security guidelines, as well as the disqualifying conditions (DC) and mitigating conditions (MC) under each guideline. In evaluating the security worthiness of an applicant, the administrative judge must also assess the adjudicative process factors listed in ¶ 6.3 of the Directive: nature and seriousness of the conduct and surrounding circumstances; frequency and recency of the conduct; age of the Applicant; motivation of the applicant, and the extent to which the conduct was negligent, wilful, voluntary, or undertaken with knowledge of the consequences involved; absence or presence of rehabilitation; and probability that the circumstances or conduct will continue or recur in the future. The decision to deny an individual a security clearance is not necessarily a determination as to the loyalty of the applicant.[(36)] It is merely an indication the applicant has not met the strict guidelines the President and the Secretary of Defense have established for issuing a clearance.

CONCLUSIONS

Guideline M--Information Technology

The government failed to make its case against Applicant under Guideline M (misuse of information technology systems). The government introduced no evidence that Applicant's downloading of software for use on his personal computer was a violation of government (USAF) or university policy. Information Technology Disqualifying Condition (IT DC) E2.A13.1.2.3. (*Removal (or use) of hardware, software or media from any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations*) does not apply. Applicant received the disks from the software custodian. Applicant was unsure if there was a policy or if so, what it was. These activities occurred from about 1985 until 1996. In these early years, computer policies were new, or not even developed. The internet came along later in this time frame. Applicant used the software to produce research for the USAF. He derived no pecuniary benefit. To argue that his wanting to use the programs at home is somehow a personal gain flies in the face of the current government practices of allowing, and even encouraging, employees to work at home.

The use of a government computer for personal use was approved by the USAF, which set up an unclassified "open computer" for employees to use to check e-mail, and for other personal business. Applicant's sending a picture of himself over this computer to his home computer does not violate any policy. Again, no policy was produced into evidence. This conduct was 12 or more years ago. I conclude Guideline M for Applicant.

Guideline K--Security Violations

The government established its case against Applicant under Guideline K (security violations.) Security Violations Disqualifying Condition (SV DC) E2.A11.1.2.1. (*Unauthorized disclosure of classified information*) is applicable because in 2003, Applicant twice sent classified information to his employer's customer using unclassified e-mail transmissions.

Security Violations Mitigating Conditions (SV MC) include actions that: SV MC E2.A11.1.3.1. (*were inadvertent*), SV MC E2.A11.1.3.2. (*were isolated or infrequent*), and SV MC E2.A11.1.3.3. (*were due to improper or inadequate training*.) Applicant did not knowingly send the classified information. When reviewing his submission before sending it, the program manager and security officer of the company failed to identify the classified information. It occurred right before Christmas holidays when employees were rushed to finish projects because the company closed down between Christmas and New Years. After the two incidents, Applicant was given additional training, given additional staff, and the process of forwarding information to the customer was changed to using couriers or a secure fax machine. I conclude Guideline K for Applicant.

Guideline E--Personal Conduct

The government established its case under Guideline E. Personal Conduct Disqualifying Condition (PC DC) E2.A5.1.2.1. (*reliable, unfavorable information provided by associates, employers, coworkers, neighbors, and other acquaintances*), 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*), and PC DC E2.A5.1.2.5. (*a pattern of dishonesty or rule violations, including violation of any written or recorded agreement made between the individual and the agency*) apply because when placed in a stressful or potentially embarrassing situation, Applicant filed a false claim with the OSI, went back a second time to give more false information, and the USAF never discovered these acts while Applicant was on active duty. Even more egregious is Applicant's failure to advise his wife of his contacts with foreign women until nine years after the conduct ended. His willingness to ignore the truth for his own benefit and his failure to acknowledge his previous falsifications by denying them renders him untrustworthy and a security risk. Contacting Eastern Bloc women in hopes of establishing any type of relationship, while holding a security clearance, further demonstrates Applicant's unreliability and questionable judgment. If this conduct was known, it certainly would have affected his personal and professional standing in the community, so he lied about it.

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*) does not apply, nor does PC MC E2.A5.1.3.3. (*The individual made prompt, good-faith efforts to correct the falsification before being confronted with the facts.*) Applicant filed a false investigation report and only disclosed the truth of his actions under threat of a polygraph exam, some eight years after the fact. He took nine years to reveal his activities to his wife, after he received the SOR. And, he initially disclosed this information to a daughter, not his wife. This is conduct as recent as nine months ago.

The other mitigating conditions provided under the Directive do not apply. He did not voluntarily correct the false information previously provided, there is no evidence that he received improper or inadequate information, and he admitted lying to the OSI rather than tell the truth. He violated his oath as an officer in the USAF, and he violated the sacred trust given to him by his wife. Consequently, I conclude Guideline E against Applicant.

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 eligible for a security clearance."[37]

"Available, reliable information about the person, past and present, favorable and unfavorable, should be considered in reaching a determination."[38]

In evaluating Applicant's case, in addition to the disqualifying and mitigating conditions, I also considered the "whole person" concept in evaluating Applicant's risk and vulnerability in protecting our national interests.[39] I considered his age (47), his education, his military service, his employment, and what might motivate him to be less than truthful. Applicant filed a false police report with federal investigators, in an effort to avoid the embarrassment of exposing his conducting clandestine contacts with women from an Eastern Bloc country. This violated his oath as an officer of the USAF. This is problematic because candor with the government about a person's negatives is the crux of a trustworthiness determination. If a person discloses the adverse information about himself, then he may be trusted with confidential or classified information. This is a serious offense.

Applicant also violated the trust reposed in him by his wife. I consider this a grave offense. Fortunately, Applicant still has the love and support of a good woman who endured the humiliation of having to testify about very private matters between a husband and wife. Because of his fear of embarrassment and humiliation, he has subjected his wife to unnecessary embarrassment and humiliation, which could have been avoided if he had told the truth.

Applicant offered the testimony of a psychologist to mitigate his conduct by testifying that Applicant's conduct can be explained away because his ethnic background is such that the fear of embarrassment and humiliation are some of the worst things that can happen to Applicant. I reject the psychologist's testimony as irrelevant and pure speculation. Fear of embarrassment or humiliation cannot justify filing a false police report as an officer of the USAF. Lying to one's spouse, no matter how embarrassing, is not justifiable. This is not a Guideline I case involving emotional, mental, and personality disorders. In fact the doctor testified that Applicant had no psychological disorders.

I am mindful of Applicant's brilliant work record. I do not question his loyalty. I do question his judgment, however, because when confronted with a challenging situation, he resorted to telling lies. The totality of the record raises reasonable and persistent doubts about Applicant's ability to protect classified information and to exercise the requisite good judgment and discretion expected of one in whom the government entrusts its interests. I conclude it is not clearly consistent with the national interest to grant or continue Applicant's security clearance.

FORMAL FINDINGS

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

Paragraph 1. Guideline M: FOR APPLICANT

Subparagraph 1.a: For Applicant

Subparagraph 1.b: For Applicant

Subparagraph 1.c: For Applicant

Subparagraph 1.d: For Applicant

Subparagraph 1.e: For Applicant

Paragraph 2. Guideline K: FOR APPLICANT

Subparagraph 2.a: For Applicant

Paragraph 3. Guideline E: AGAINST APPLICANT

Subparagraph 3.a: Against Applicant

Subparagraph 3.b: Against Applicant

Subparagraph 3.c: Against Applicant

Subparagraph 3.d: Against Applicant

DECISION

In light of all of the circumstances in this case, it is not clearly consistent with the national interest to grant or continue a security clearance for Applicant. Clearance is denied.

Christopher Graham

Administrative Judge

[1] Tr. at 131.

[2] *Id.* at 30, 32.

[3] *Id.* at 36.

[4] *Id.* at 37.

[5] *Id.* at 31-32.

[6] *Id.* at 38-39.

[7] *Id.* at 30-31.

[8] *Id.* at 41.

[9] *Id.* at 43.

[10] *Id.* at 44-46.

[11] *Id.* at 46-49.

[12] *Id.* at 50.

[13] *Id.* at 53.

14. *Id.* at 53-54.

15. *Id.* at 58-63; Government Exhibit 3 (Letter of Reprimand, dated January 19, 2004) at 1.

16. *Id.* at 60-64; 107-108.

17. *Id.* at 66-69.

18. *Id.* at 73.

19. *Id.* at 57.

20. *Id.* at 57, 99.

21. *Id.* at 100.

22. *Id.*

23. *Id.* at 136-142.

24. *Id.* at 42.

25. *Id.* at 156-175.

26. Applicant's Exhibit F (Psychological Evaluation, dated September 8, 2006) at 5-9, portions stricken at 6,8, and 9.

27. *Id.* at 192.

28. *Id.* at 205.

29. *Id.* at 206.

30. *Id.* at 207-208.

31. [0]*Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988).

32. [0]*Id.* at 527.

33. [0]Exec. Or. 10865, *Safeguarding Classified Information within Industry* § 2 (Feb. 20, 1960).

34. [0]Directive ¶6.2.

35. [0]ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002).

36. [0]*See* Exec. Or. 10865 § 7.

37. Directive ¶ E.2.2.1.

38. *Id.*

39. *Id.*