DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 09-05617
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Alison O'Connell, Esquire, Department Counsel
For Applicant: Krystal Limon, Esquire

May 4, 2011

Decision

MATCHINSKI, Elizabeth M., Administrative Judge:

Applicant engaged in cyber-sexual contacts with several women, including two Canadian citizens, from about 2001 until 2005. He had a sexual liaison with one of the Canadian women while on a business trip in 2001. Despite an expressed intent not to engage in such behavior in the future, he had online contact of a sexual nature with another woman around October 2009. Applicant's spouse is now aware of these activities, but the Personal Conduct concerns are not fully mitigated. Applicant improperly contacted some of these women through his work computer, and he was not candid about this behavior during a previous security investigation. He also did not report to security officials at work that he had committed several security infractions between 1994 and 2002, or that he had contact of a sexual nature with foreign nationals. The concerns support a whole-person assessment of questionable judgment. Clearance denied.

Statement of the Case

On March 15, 2010, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) to Applicant, detailing the security concerns under Guideline D (Sexual Behavior), and Guideline E (Personal Conduct), which provided the basis for its preliminary decision to revoke his security clearance. 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 adjudicative guidelines (AG) effective within the Department of Defense on September 1, 2006.

Applicant answered the SOR allegations on April 19, 2010, and requested a hearing to be held at least six months in the future. On August 12, 2010, previously assigned Department Counsel materially amended the SOR by deleting Guideline D and alleging the cyber sexual conduct and related matters instead under Personal Conduct. Furthermore, five security violations were added under Guideline E, which Applicant allegedly failed to report to his facility security officer (FSO). Applicant was also alleged to have misused his work computer around May 2004 to contact some of the women with whom he had engaged in cyber sex. Applicant was directed to respond to the amended SOR within 20 days of receipt. On August 24, 2010, the case was assigned to me to consider whether it is clearly consistent with the national interest to grant or continue a security clearance for Applicant. On September 9, 2010, counsel for Applicant entered her appearance, and with the agreement of the parties, I scheduled the hearing for October 8, 2010. On September 30, 2010, Applicant answered the amended SOR.

I convened the hearing as scheduled on October 8, 2010. The Government notified me of the amended SOR and submitted eight exhibits (Ex. 1-8). Exhibits 1 through 7 were admitted without objection. I sustained Applicant's objection to proposed Exhibit 8, Applicant's employer's corporate procedure for Internet use, because the effective date of the policy post-dated the issues in the SOR. Sixteen Applicant exhibits (Ex. A-P) were admitted without objection. Applicant, Applicant's spouse, and three of Applicant's coworkers, testified, as reflected in a transcript (Tr.) received on October 15, 2010.

Summary of SOR Allegations

The amended SOR alleged under Guideline E, Personal Conduct, that Applicant's program access was revoked by a Government agency in about December 2004 due in part to the information alleged in the SOR (SOR 1.a); that Applicant engaged in cyber sex with around 50 women from 2001 through 2003, including two Canadian citizens, and that he had a sexual liaison with one of these Canadian women while on business travel around 2001 (SOR 1.b); that Applicant disclosed to one of the women (SOR 1.c) that he was an aerospace engineer with a clearance in an attempt to impress her; that his spouse is unaware of his cyber sex and the sexual liaison (SOR 1.d); that he withheld the cyber sex and sexual liaison activities during a polygraph with a Government agency in October 2004

(SOR 1.e);[1] and that he failed to report his foreign contacts to his FSO (SOR 1.f). Applicant was also alleged to have reported during his interview with another Government agency, but not to his FSO (SOR 1.h), that he had violated security procedures by failing to report that he had twice brought his cell phone into the building (SOR 1.g(1)), had failed to mark classified documents properly (SOR 1.g(2)), had brought six homemade music compact disks into the office between 1999 and 2002 without having them scanned by security (SOR 1.g(3)), had removed a classified disk while working abroad in 1997 (SOR 1.g(4)), and had failed to protected classified information in an area where uncleared persons were working in 1994 (SOR 1.g(5)). Furthermore, Applicant was alleged to have communicated with some of the women with whom he had cyber sex through his work computer without authorization on three to six occasions around May 2004 (SOR 1.i).[2]

Findings of Fact

Applicant denied the allegations in the amended SOR. After considering the pleadings, exhibits, and transcript, I make the following findings of fact.

Applicant is a 49-year-old operations manager for a defense contractor. (Ex. 1.) He seeks a security clearance for his duties. He previously held a Top Secret security clearance with sensitive compartmented information (SCI) access until December 2004, when his special access was revoked for the conduct alleged in the amended SOR. (Ex. 3; 7.)

Applicant served honorably as an electronics technician in the U.S. military from July 1980 to December 1990. He held a security clearance for his military duties from 1982 to 1990. (Tr. 92.) From December 1989 to December 1990, he was deployed to the Middle East. He was awarded a Navy Achievement Medal for his contributions. (Ex. P.) He was married to his first wife from 1982 to 1990, and has a daughter from that marriage. (Ex. 1; 2.) After earning his bachelor's degree in electronic engineering technology, Applicant began working as an engineering support specialist for a defense contractor in August 1991. (Ex. 3; N; P; Tr. 93.) In December 1991, Applicant was assigned to a sensitive project onsite in foreign country X. He was granted special program access, and he signed

[1]The Government amended the SOR to add SOR 1.e, "You withheld information regarding your activities as set forth above in subparagraph 1.b during polygraph testing with another government agency in October 2004." However, Applicant was then asked to specifically respond to the following SOR 1.e: "You withheld information regarding your activities as set forth in subparagraph 1.b during an interview with another government agency in October 2004." There is a material discrepancy between whether Applicant lied during polygraph testing and during an interview that may or may not have been administered during the course of a polygraph examination. During an October 2004 interview, Applicant apparently revised some information about his cyber sex encounters from what he had provided during the October 2004 polygraph. *See* Ex. 3. Department Counsel did not attempt to clarify the mistake apparently made by her colleague when redrafting the allegation for Applicant's response.

[2]Department Counsel clarified at the hearing that SOR 1.i alleges communications with some of the women through unauthorized use of his work computer, as set forth initially in the amendment. When the allegation was redrafted for Applicant's response, the Government mistakenly duplicated the concern in SOR 1.c and omitted the alleged unauthorized use of the work computer.

a Lifetime Nondisclosure Agreement agreeing that he would not disclose certain elements of his job, specific program information, or links to specific government agencies. (Ex. 3.)

While living and working in country X, Applicant met, and in June 1993 married, his current spouse, a native citizen of country X. Applicant and his spouse have two children, who are dual citizens of country X and the United States. (Ex. 1; 2; Tr. 72.)

As required of all individuals with restricted program access, Applicant received annual security briefings from his employer on his security responsibilities. During those briefings, Applicant was reminded of his continued responsibility to protect classified information and to report to security any incident that might impact program security. (Ex. 5; Tr. 132-33.) In October 1993, Applicant verified by signature that he had reviewed the security guidelines handbook and his employer's polygraph policy as applied to restricted program briefed employees. (Ex. 6.) In 1994, Applicant left some classified documents in the open in the facility where uncleared persons could have accessed them. (Ex. 3; Tr. 123-24.) There is no evidence that the classified material was accessed by an uncleared person, however.

Applicant underwent polygraph testing in 1995 and 1996 with three different examiners. He volunteered that he had disclosed to his spouse certain aspects of his job responsibilities, specifically the meaning behind a designated program patch affixed to his jacket. However, Applicant's spouse testified that she commented about the badge based on public information, and that Applicant never commented about the program to her. (Tr. 77.) The patch became classified because of its link to a generic systems patch he also displayed. Applicant claims he did not realize that he could not display the two patches together. (Ex. 4.) Applicant felt demeaned by his polygraph experience, and he and his spouse agreed thereafter to maintain a "don't ask, don't tell" policy. (Ex. 3.)

In 1997, while on business in Europe, Applicant inadvertently removed from a secure area a floppy disk containing highly classified information. He went to lunch with the disk in his pocket. He brought it back after lunch and informed security onsite. (Ex. 4; Tr. 121-22.)

After almost five years as a maintenance training engineer, Applicant became a system operator in April 1998. In July 1999, apparently as a result of a corporate acquisition, Applicant began working for his current employer as a system training engineer on the project. (Ex. N; O.) Applicant was retested by a polygraph examiner in October 1999, and he retained his security clearance and special access. (Ex. 3.)

Between 1999 and 2002, Applicant brought six homemade music compact disks into his classified work area without having them scanned by security personnel. Applicant was unaware at the time of any prohibition against bringing compact disks into the building provided they were not inserted into a government-sponsored computer and did not leave the facility. (Ex. 3; Tr. 118-21.)

Around 2001, Applicant became involved in online games of a sexual nature. He now recalls that over the next few years, through 2003, he had online cyber sex with several women. While he now recalls he had contact via instant messaging with five anonymous women on no more than 20 occasions (Tr. 95.), he had estimated in October 2004 that in "a worse-case scenario" he had 50 to 100 cyber sex encounters with over 50 different women. (Ex. 3.) He informed some of his online contacts that he was an aerospace engineer, and that he held a security clearance, although it was to avoid further questions about his job and not with the intent to impress them. (Tr. 107-08.) In October 2001, he had a sexual liaison with one of the women, a married Canadian teacher, with whom he had developed an online relationship since May 2001. (Tr. 102; 146.) He engaged in telephone sex with her twice and provided her with some personal data. She spent the weekend with him while he was on a business trip to the United States. The following weekend, he visited her in Canada. (Ex. 3; 4.) When they met, Applicant wore his jacket containing the two patches which were later determined to be classified. (Ex. 3.) Applicant informed his local security office that he traveled to Canada during this business trip (Ex. 4.). But there is no evidence that he told the security office of the sexual liaison with the foreign national. In 2002, Applicant began an online personal relationship with a social worker in Canada. While they never met in person, he became "emotionally connected" to her, and they had online contact of a sexual nature. (Ex. 3; 4.) He did not report his contact with this Canadian citizen to security officials at work. (Tr. 113.)

Applicant had an online friendship with a married U.S. homemaker that eventually became intimate. Plans to meet her in person in the United States fell through due to hurricane activity. He stored over 100 nude phones of her on his personal computer, engaged in cyber and phone sex with her in 2004, and received locks of her hair.[3] He disclosed to her that he had a security clearance (Ex. 3; Tr. 138, 142.), and she jokingly referred to him as "Special Agent Man" and "Gov Man." (Ex. 3; Tr. 141-42.) Applicant met her through his duties as host of an online radio show from 2004 to 2008, and not from his online gaming activities. (Tr. 78, 102, 137.)

Sometime between 2003 and 2004, Applicant brought his cellular phone with him into the workplace on two occasions when he should have secured it in the car. As soon as he realized he had the phone on him, he left the premises and put the phone in his vehicle. (Tr. 115.) Applicant did not inform security officials of his inadvertent violations of security procedures. Applicant believed that under facility policy, a note of this minor security infraction would have been placed in his record for one year and then purged if no further infractions. Applicant gave no specific reason for not reporting the infractions other than that he thought he handled it in an acceptable manner at the time. (Tr. 116.)

In at least May 2004, he used an unclassified work computer without authorization on six occasions to contact women with whom he had online contact of a sexual nature.

[3]Applicant testified that ninety percent of their contacts involved non-sexual matters, and that "on a couple of occasions it crossed the line into a sexual type conversation and then that was it." (Tr. 138.) However, he previously acknowledged when he appealed the revocation of his special access in March 2005 that he had 100 nude photographs of her stored on his personal computer. (Ex. 3.) Their intimate relationship cannot reasonably be characterized as limited to a couple of sexual type conversations.

(Ex. 3.) He denies that the content of his instant messages had a sexual nature. It was "just conversation, how are you doing, what's going on, what are you doing." (Tr. 149.) Applicant does not consider this use of the work computer to be unauthorized because there were no specific guidelines regulating access to the Internet through his particular computer at the time. (Tr. 124-25.) Applicant corresponded via instant messaging on this unsecured computer during breaks. (Tr. 125-26.) He knew access to instant messaging was permitted because he had authorized use for school studies and that access to pornographic sites was prohibited. (Tr. 148.)

Only two of the women (the married Canadian teacher and the married U.S. homemaker) knew his location in foreign country X (Tr. 139), and few of the women knew he held a clearance. (Ex. 3.) Applicant's spouse testified that she "pretty much knew" that he engaged in activities of a sexual nature online at the time. (Tr. 68.) They argued over his online activities, which he saw as fairly innocent. (Tr. 79.)

In October 2004, Applicant underwent another polygraph examination, which he understood was a routine, five-year update for his special access. (Tr. 128.) Apparently during a polygraph concerning counterintelligence issues (Tr. 98), Applicant reported two foreign national contacts from on-line gaming activities. He admitted that he had online contact of a sexual nature as well with women from the United States that he maintained through instant messaging. He volunteered that he had telephone contact with two Canadian women, including one woman with whom he had an affair while on his business trip in October 2001. Applicant indicated that but for three instant messages sent from an unclassified computer at work in May 2004, he corresponded via his home computer. Applicant acknowledged that his spouse was unaware of his sexual activities. Given the opportunity to explain himself in detail during a subsequent interview, Applicant indicated that he had 50 to 100 sexual encounters with over 50 different women during online games, had engaged in phone sex twice with the Canadian with whom he had the affair, and furnished personal data to her. He acknowledged that he had misused his unclassified computer at work at least six times for these online contacts. And in response to counterintelligence inquiries, Applicant disclosed that he had failed to report to his security officer that he had brought his cell phone into his work without authorization on two occasions, had failed to properly mark classified documents that he generated (Tr. 117), had brought six music compact disks into work without having them scanned, had inadvertently removed a classified disk from the worksite in 1997, and had failed to protect classified information in an area where uncleared persons worked in 1994. (Ex. 3.)

Applicant's SCI access was suspended on October 22, 2004, and then revoked on December 9, 2004 (Ex. 5), for withholding information during security processing, foreign influence and failure to report continuing contact with foreign nationals, sexual behavior showing poor judgment, negligent security practices, and his disclosure of job-related information to foreign nationals. Applicant appealed the revocation, contending in part that he had never been trained or briefed on the security standards set forth in Director of Central Intelligence Directive 6/4. Applicant indicated that while those persons to whom he disclosed his profession of aerospace engineer seemed impressed, he did not freely give out information about his occupation or location. As for the concerns that he only provided

additional details when confronted, Applicant denied he intentionally concealed any information. He withheld details which he believed had nothing to do with his national security work. Moreover, he was not allowed to explain his activities, and was told to admit that he engaged in activity if he was 51% assured that it took place. Having had time to reflect, Applicant revised his estimate of cyber sex encounters "to no more than twenty occasions with no more than five characters." The decision to revoke his SCI access was upheld, and Applicant was informed that he could reapply for program access in September 2006. (Ex. 3.)

With the revocation of his special access, Applicant could no longer work on the program or remain a resident in country X without a job since he was in the country on a work visa. He uprooted his family and they moved to the United States in February 2005 ("We were unceremoniously dumped at the airport in L.A. with nothing. I had no job, I had no car, I had no place to live. We had nothing."). (Tr. 104.) Applicant was not given the usual 30 to 60 days of coverage on an overhead job number while he looked for another assignment in the company because of the circumstances under which he lost his overseas placement. (Tr. 104.) Applicant had to explain to his wife why they were forced to leave her native country. He told his spouse that he had an online relationship with the Canadian social worker, which she apparently had known about since "early in 2000" (Tr. 73), and that he had engaged in cyber sex. However, he kept silent about his extramarital affair with the Canadian teacher. (Ex. 3; 4; Tr. 72.) He hid it because "that's what guys do" (Tr. 103), and he "could not bear the spectacle or the idea of causing more hurt to her at that time." (Tr. 105.) Applicant testified that his spouse knew about the U.S. homemaker because the two women "exchanged recipes and things like that." (Tr. 139.)

Over the next few months, he looked for other employment opportunities within the company. (Ex. F.) In April 2005, Applicant began working as a command controller on a satellite program, which necessitated moving his family to their present locale. He continued to pursue ways of increasing his value to his employer, as he had in the past. (Ex. K; P) In April 2006, he was promoted to operations controller. (Ex. K; N.) In January 2008, he assumed his present position as operations manager. (Ex. K; M; N.)

On February 2, 2009, Applicant completed an Electronic Questionnaire for Investigations Processing (e-QIP) for a Secret-level security clearance. (Tr. 106.) He disclosed that his SCI access had been suspended for one year from January 2005. (Ex. 1.) On March 19, 2009, Applicant was interviewed by an Office of Personnel Management (OPM) investigator about his past relationships with foreign nationals. He acknowledged his affair in 2001 with the Canadian teacher, which remained secret to his family and friends, including his spouse. He indicated that he would inform his spouse about the affair if his continued concealment prevented him from getting a security clearance. Applicant maintained that he had told his spouse about his online relationship with the Canadian social worker, with whom he claimed to have contacted only six times since 2002. Applicant attributed his sexual contacts to him and his wife leading separate lives at the time. He was working a lot and she had her activities, family, and friends. He denied he would be subject to blackmail because of these relationships, or that he intended to have another affair or Internet relationship because of the price he and his family had already

paid. Applicant explained his security infractions, which were inadvertent, and he continued to maintain that the suspension of his clearance had been unjustified. (Ex. 4.)

On December 16, 2009, Applicant indicated to DOHA that he did not see any good that would arise from informing his spouse of his marital indiscretion. However, if it remained the only hurdle to overcome for him to be granted a clearance, he would tell her of the affair. (Ex. 4.) On March 15, 2010, DOHA issued the original SOR to Applicant alleging in part that his spouse was unaware of his cyber sex or his extramarital activities or both. Applicant received the SOR on April 1, 2010. On April 15, 2010, he informed his spouse of his affair with the Canadian teacher.[4] (Tr. 67.)

Applicant's marriage has improved significantly since they moved to the United States. (Tr. 68.) Applicant's spouse does not believe that Applicant is continuing to hide things from her. He has exhibited remorse to her and "a big turnaround in his behavior." (Tr. 70.) Specifically, he spends his time outside of work with her and their children. He is no longer involved in online gaming activities or in the online radio show. (Tr. 78, 102.) Applicant found that the radio show was "too much of a magnet for these types of people who liked to engage in this kind of activity." (Tr. 103, 140.)

At his October 2010 hearing, Applicant acknowledged that he last engaged in cyber-sexual activity "roughly one year ago," through Internet chat with one of the listeners of his radio show. (Tr. 150-51.) He had helped her through a difficult part of her life and she "found him very impressive and very this and very that. We got carried away, crossed the line, but [this conduct is] not to be repeated." (Tr. 151-53.) Applicant denies, and there is no evidence that he engaged in any cyber-sexual activities after 2005 until this latest episode around October 2009. Applicant expressed remorse for his cyber-sexual activities and extramarital affair, and for "not explaining those and confessing to those earlier than I had." (Tr. 130-31.) He believes that he and his family paid a "tremendous price" and he does not intend to engage in similar conduct in the future.

Applicant's present coworkers fully support his application for a security clearance. (Ex. A; C-D; G; I; Tr. 45-48, 52-55, 61-63.) A member of Applicant's team for over the past two years has known him to be loyal to their mission, unbiased, flexible in scheduling matters, competent, and trustworthy. She reports that Applicant is "viewed as a good family man away from work." (Ex. A.) A peer of Applicant's, who serves as manager of an engineering group, has worked with Applicant on a wide range of program and personnel

[4] Concerning his decision to inform his spouse in 2010 about his extramarital affair, he responded:

> I decided to tell her because although my ultimate goal is to be able to get my special access back, once I was eligible again, which I am based on the Statement of Reasons, the agency put on an additional burden to me that I had to be granted a DoD secret clearance to show that I could get a clearance before they would consider my special access. And then when I applied, I got this correspondence from the Government, essentially the Statement of Reasons, which made it very clear that until the Statement of Reasons—the items on the Statement of Reasons could be cleared, they obviously weren't going to grant me a security clearance. (Tr. 106.)

issues. Applicant "kept his cool" during an unexpected loss of telemetry in October 2008 and played "a critical role" in the response and recovery from the system anomaly. This manager is aware of the SOR allegations,[5] which are not in character with his experience of Applicant as a dedicated professional with high ethical and personal standards. (Ex. C; Tr. 45-48.) A mission planning manager also aware of the SOR allegations has found Applicant to be patient as a mentor, a thorough planner, and fair and honest. When a mistake by a member of Applicant's team led to significant downtime for the program in August 2009, Applicant treated it as an opportunity to improve training for the entire operations group rather than focus blame on the culpable employee. (Ex. D; Tr. 53-54.) A manager, who works for the astrophysical laboratory contracted to operate the satellite system, opines that Applicant is committed to team success in all facets of flight operations. (Ex. B.) Applicant was nominated for a company president's award for his contributions to the satellite program in 2009. (Ex. J.) For the 2007 (Ex. O) and 2008 (Ex. N) ratings periods, his performance was rated as "exceeds performance requirements." For 2009 (Ex. M), his overall performance was rated as "meets performance requirements."

Policies

The U.S. Supreme Court has recognized the substantial discretion the Executive Branch has in regulating access to information pertaining to national security, emphasizing that "no one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988). When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the adjudicative guidelines. In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially disqualifying conditions and mitigating conditions, which are required to be considered 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, these guidelines are applied in conjunction with the factors listed in the adjudicative process. The administrative judge's overarching adjudicative goal is a fair, impartial and commonsense 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 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. 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 to obtain a favorable security decision.

[5] These coworkers were apparently not informed until shortly before Applicant's October 2010 hearing on his clearance eligibility. (Tr. 47, 56.)

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 that 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 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

Personal Conduct

The security concern about personal conduct is set out in Guideline E, 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.

Personal conduct concerns arise because of Applicant's inappropriate conduct while on business and misuse of a work computer to maintain contacts with online sexual partners; unrelated security infractions; and concealment of information that could negatively impact his personal, professional, or community standing. Applicant estimated in an October 2004 polygraph interview that he had engaged in cyber sex with over 50 women between 50 and 100 times through online gaming activities (SOR 1.b). In March 2005, in response to the revocation of his special access, he revised his estimate to no more than five anonymous women on 20 occasions. Cyber sex involving 50 women would tend to suggest a problem controlling the behavior that may not be so if only five women were involved. While some overestimation is to be expected, it is difficult to believe that Applicant would have volunteered that he had cyber sex with over 50 women if he was involved with only a handful. That said, private sexual contacts between consenting adults, whether in person or online are not of concern, unless they reflect questionable judgment or create a vulnerability to exploitation, manipulation, or duress. *See* AG ¶ 16(e), "personal conduct, or concealment or 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 displayed poor judgment by providing personal information about his location and clearance status to at least two women, one of whom was a foreign national

(SOR 1.c). Even if he was unaware of any specific prohibition against informing others about his security clearance, and he revealed his clearance status to avoid further questions about his job, he heightened his risk of vulnerability through this lack of discretion. Moreover, Applicant's rendezvous with a Canadian national while he was on a business trip to the United States for his employer in October 2001 was inconsistent with the good judgment and discretion required of those persons holding special access. Apparently, he informed his site FSO that he had traveled to Canada. Applicant's current employer has no record that Applicant reported any foreign contact. (Ex. 7.) Accounting for the possibility that the onsite FSO failed to document Applicant's foreign contact, there is no evidence to indicate that Applicant revealed to his employer that he had a sexual liaison with the Canadian citizen. It is noted that he never reported his contact with the Canadian social worker to his employer. Furthermore, Applicant concealed his marital infidelity from his spouse until April 2010. AG ¶ 16(e) is implicated because of his inappropriate conduct while on a business trip and his concealment of the sexual liaison.

In light of Applicant's denial, the Government has the burden of establishing by substantial evidence that Applicant deliberately withheld information concerning his cyber sex and affair during polygraph testing in October 2004 (SOR 1.f). Available information substantiates that during the polygraph testing process, Applicant reported two foreign national contacts through online gaming; that he had contact through instant messaging, including on three occasions from work, with some foreign nationals as well as some U.S. women with whom he had cyber-sexual relations; that he revealed his occupation, clearance status, and location to at least two of the women; and that he had telephone contact with one Canadian, and telephone contact and a sexual liaison while on business travel with another Canadian. The Government agency that revoked Applicant's special access also reported that Applicant only provided details when confronted. Furthermore, during his subsequent interview, Applicant indicated that he had 50 to 100 cyber sex encounters with over 50 different women; that he had withheld information regarding his relationships during the polygraph; that when he met the Canadian citizen with whom he had a sexual liaison, he wore the jacket with patches later determined to be classified; and that he used a computer at work on at least six different occasions to contact his online sexual partners. (Ex. 3.) Applicant submits that he volunteered the information about his affair with the Canadian teacher during the polygraph, when he was not asked lifestyle questions. (Tr. 111.) He maintains he was not allowed to explain until his interview, when he was told to disclose any wrongdoing, and any conduct if it was more likely to have happened than not in accord with what Applicant described as the 51% rule. (Tr. 99.) Consequently, he overestimated the extent of his sexual contact during that interview.

No report from the polygraph examiner was made available for my review, and I cannot speculate as to the questions asked or their context. That said, the evidence tends to show some minimization by Applicant during polygraph processing as to the extent of his cyber-sexual activities. When he appealed the revocation of his special access, Applicant did not dispute that he had withheld information regarding his cyber sex relationships during the polygraph examination ("At times I have not disclosed information that I believed at the time had [sic] were outside the bounds to a CI polygraph i.e., the information had nothing to do with my work of national security . . . the information pertained to my personal

life."). (Ex. 3.) AG ¶ 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," applies.

As for using instant messaging at work to correspond with some of the women with whom he had cyber sex (SOR 1.i), Applicant asserts that the content of his messages was not sexual in nature, and that he used the computer while on breaks. Since the computer was apparently not approved for processing of classified information, his employer could have authorized limited Internet access and instant messaging for legitimate purposes. Yet it is difficult to see where correspondence with online sex partners could be viewed as legitimate, even if the content did not cross the line. Instant messaging, unlike web-surfing, is a two-way conversation. Given the sexual nature of his relationships with these women, Applicant had no assurance that their messages back to him would be free of sexual innuendo or comment. Even if there was no express prohibition against instant messaging for benign personal reasons, this misuse of the computer falls within AG ¶ 16(d), which provides in pertinent part:

> (d) credible adverse information that is not explicitly covered under any other guideline and may not be sufficient by itself for an adverse determination, but which, when combined with all available information supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the person may not properly safeguard protected information.

Concerning Applicant's admitted violations of security procedures (SOR 1.g), Applicant removed a highly classified disk from the worksite while on business in Europe in 1997, but by all accounts, his conduct was inadvertent and he reported his violation. As for him taking homemade music disks into work, Applicant assumed it was permissible provided he did not then take the disks home and they were not inserted into a work computer. As of 2009, company policy expressly stated that homemade compact disks were to be confiscated and destroyed. (Ex. 6.) Without evidence establishing that this security policy was in place between 1999 and 2002, I cannot conclude that Applicant knowingly violated a security procedure concerning bringing music CDs into work. In contrast, Applicant had been briefed on his security responsibilities. He knew or should have known that he had to mark self-generated classified documents at the appropriate level (SOR 1.g(2)). Moreover, while he may have inadvertently brought his cell phone to the workplace on two occasions between 2002 and 2004 (SOR 1.g(1)), he knew at the time that a memo would likely be placed in his file if he reported his violation. (SOR 1.g(1)). His failure to report his violation was intentional and an exercise of poor judgment. His security infractions are now dated, but together with the other conduct of concern under Guideline E (his minimization of his online cyber-sexual activities during polygraph processing in 2004, his involvement in cyber sex with foreign nationals, his sexual liaison with a Canadian citizen while on a business trip for his employer, his concealment of that affair from his spouse until after he received the SOR, and the poor judgment exhibited by

instant messaging his online sex partners at work), AG ¶ 16(c) is clearly established. That disqualifying condition is as follows:

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

Concerning potential factors in mitigation, AG ¶ 17(a), "the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts," partially applies. Applicant disclosed in his 2004 interview more extensive cyber-sexual activity than he had revealed during polygraph processing. This rectification is undermined somewhat by his subsequent efforts to minimize the seriousness and extent of his cyber-sexual activity, i.e., it involved in retrospect only five different women; he was authorized to use instant messaging at work and his contact with his cyber-sexual partners through the work computer did not have sexual content. *See* Ex. 3; Tr. 100, 125. So AG ¶ 17(a) is not entitled to controlling weight.

AG ¶ 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," is implicated in part. Since Applicant began his present assignment in August 2005, he has not violated security procedures by bringing his cellular phone to the worksite without authorization, by bringing homemade music CDs into work (which has been prohibited since 2009 if not before then), by removing any classified information from secured premises or otherwise failing to protect classified information, or by failing to mark classified documents properly. So much time has passed without recurrence to mitigate the judgment concerns raised by the conduct alleged in SOR 1.g. Applicant's failure to report known security infractions to his employer (SOR 1.h) is considered ongoing, however, in light of evidence showing that his employer has no known record of him having violated security procedures. Also, while ten years have passed since his sexual liaison with the Canadian teacher during the October 2001 business trip, even if I accept that he notified his onsite FSO in 2001 of the foreign contact, available information does not show that he reported the sexual nature of his contact or that he ever told his employer of his contact with other foreign nationals, including the Canadian social worker with whom he had cyber sex. Similarly, while he acknowledges that he contact some of his online sexual partners through a work computer, his failure to acknowledge his lack of good judgment in that regard precludes me from applying AG ¶ 17(c) to that conduct, despite the passage of time without recurrence.

Applicant has taken significant steps, albeit some very belated, to reduce his vulnerability to exploitation, manipulation, or duress by informing his spouse about his marital indiscretions. *See* AG ¶ 17(e) (stating, "the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress"). When his special

access was revoked in 2005, he informed his spouse about his cyber-sexual activities, but not of his extramarital affair. He did not want to tell her "simply because that is what guys do." He also did not want to deal with the ramifications that held for his marriage at the time. (Tr. 103.) After he received the SOR, he told his spouse about his affair. The coworkers who testified on Applicant's behalf were informed of the allegations in the SOR, although not until a few weeks (Tr. 49), and in one case one week (Tr. 56.) before Applicant's October 2010 hearing. Because his spouse is aware of the affair and of his other marital indiscretions, Applicant has largely mitigated concerns alleged in SOR 1.d. of his vulnerability.

However, by engaging in cyber-sexual contact around October 2009, with a listener of his Internet radio show, Applicant undermines substantially his case for mitigation under AG ¶ 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." Applicant submitted in appeal of his March 2005 revocation of his special access that besides his family, having program access was "the most important and precious part of [his] life." (Ex. 3.) He indicated to an OPM investigator in March 2009 that he would never have another affair or Internet relationship again because he and his family had paid a heavy price by having to move to the United States. (Ex. 4.) The Internet chat occurred off-duty, between consenting adults. It seemingly does not make him vulnerable because his spouse knows about it. Nonetheless, it occurred after he had terminated his radio show because it raised the potential for cyber-sexual activities. Doubts about his judgment and his willingness or ability to stand by his commitments persist.

Furthermore, while Applicant's candor about this latest incident weighs in his favor, it does not completely mitigate the Personal Conduct concerns raised by his years of concealment of his extramarital affair from his spouse, his minimization of his sexual indiscretion during polygraph processing, and his failure to comply with reporting requirements concerning matters that could impact his clearance or access eligibility. Applicant testified that he now knows that he has to report himself "if a mistake occurs." (Tr. 130.) But he also continues to justify his failure to report (e.g., "Specifically [the Canadian social worker], she was not ever reported, but that was never a physical contact") (Tr. 113.); he thought he handled the cellular phone matter "in an acceptable manner at the time" (Tr. 116); concerning his use of the work computer to send instant messages to his sexual partners, "I know for a fact that using that particular computer for personal use was fine because many people did it" (Tr. 125.)).

AG ¶ 17(f), "the information was unsubstantiated or from a source of questionable reliability," applies only to SOR 1.g(3), bringing six homemade music compact disks into the office between 1999 and 2002 without having them scanned. Applicant indicated in March 2005 that he was unaware of any prohibition at that time. The Government's evidence to the effect that homemade compact disks will be confiscated by Applicant's employer is from a 2009 annual security refresher briefing, well after the conduct at issue.

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 his conduct and all relevant circumstances in light of 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.

Applicant has earned the respect of those coworkers in his current job assignment for his dedication, ethical behavior, and flexibility as a manager. The evidence of Applicant's value to his employer is undisputed, but it is not enough to overcome the Personal Conduct concerns, which when taken as a whole, show questionable judgment, untrustworthiness, and unreliability on Applicant's part. He has appropriately expressed remorse for his personal indiscretions ("it was the wrong thing to do") and for his failure to report. (Tr. 130-31.) Yet he continues to see himself as victimized by women attracted to cyber-sexual activities ("I should have been stronger and [not] to let myself get lured into those types of activities") (Tr. 130.); by a polygraph process that he found demeaning, did not allow him to explain, and pressured him into exaggerating (Ex. 3; Tr. 100); by an employer who dispatched him from his overseas assignment without any overhead coverage ("we were unceremoniously dumped at the airport in L.A. with nothing") (Tr. 104); and even by a Government that has placed a stipulation on him to obtain a security clearance that he believes is not normally required for program access. (Tr. 143.) He has yet to fully mitigate the Personal Conduct concerns for the reasons already noted.

Formal Findings

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

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

Subparagraph 1.h:	Against Applicant
Subparagraph 1.i:	Against Applicant

Conclusion

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 Applicant eligibility for a security clearance. Eligibility for access to classified information is denied.

_____
Elizabeth M. Matchinski
Administrative Judge