DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 09-07741
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: David Hayes, Esq., Department Counsel
For Applicant: *Pro se*

November 19, 2010

Decision

RICCIARDELLO, Carol G., Administrative Judge:

Applicant mitigated the security concerns under Guideline B, Foreign Influence, but failed to mitigate the Government's security concerns under Guideline E, Personal Conduct. Applicant's eligibility for a security clearance is denied.

On July 7, 2010, the Defense Office of Hearings and Appeals (DOHA) issued Applicant a Statement of Reasons (SOR) detailing security concerns under Guideline E and B. On September 7, 2010, DOHA filed an amended SOR. The actions were 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 for SORs issued after September 1, 2006.

Applicant answered the SORs in writing on August 4, 2010 and September 15, 2010. Applicant requested a hearing before an administrative judge. The case was assigned to me on September 13, 2010. DOHA issued a Notice of Hearing on

September 21, 2010. I convened the hearing as scheduled on October 20, 2010. The Government offered Exhibits (GE) 1 through 5. Applicant did not object and they were admitted into evidence. The Government requested administrative notice be taken of certain facts relating to India as contained in Hearing Exhibit (HE) I. Applicant did not object and I took administrative notice of the documents. Applicant testified on his own behalf. Applicant did not offer any exhibits. DOHA received the hearing transcript (Tr.) on October 27, 2010.

Findings of Fact

Applicant denied the allegations in the SOR ¶¶ 1.a and 1.b and admitted the allegations in ¶¶ 2.a, 2.b, and 2.c. After a thorough and careful review of the pleadings, exhibits, and testimony, I make the following findings of fact.

Applicant is 43 years old. He married in 1994. He was born in India and became a naturalized United States citizen in 2003. His wife is a citizen of the United States. His children, ages 12 and 10, are both United States citizens. Applicant holds a bachelor's degree and two master's degrees. Applicant has been employed by a federal contractor since August 2008. He has a Top Secret security clearance.[1]

Applicant stated that work was assigned to him by his manager, from August 2008 until approximately January 2009, when his manager went on maternity leave. He explained once his manager left for maternity leave he was not assigned work. [2]

Applicant stated that "now and then" he accessed the internet at work, usually for 15 minutes every two hours.[3] He stated most of his internet usage was on approved sites. He consistently did this over a two and a half month period. He estimated that out of a 40-hour work week during this period, he would work an average of about seven to eight hours, five hours would be used to view the internet, and the remaining 27 hours he had no work to do, so he read work-related material. He charged his government client for the full 40-hour workweek, even though he did not do work for them. He admitted he charged the government client for work he did not do. He explained he was a salaried employee of his company and this was the only way he could get paid. He did not have a reasonable explanation for charging his government client for work he did not do, other than to state that it was his company's fault because they did not give him any work. Applicant stated he did not know that he should not charge customers when work was not performed.[4]

[1] Tr. 36, 39-40, 94-97.

[2] Tr. 22-23.

[3] Tr. 23-24.

[4] Tr. 28-35, 46-52, 99-101-102.

In late March 2009, an investigation was started by his company because they were suspicious that Applicant was spending an inordinate amount of time on the internet. His government-owned computer utilized an unclassified network. Their investigation revealed that numerous sites Applicant accessed from his company's account were inappropriate in the workplace. The investigation revealed one sample representing a one hour and fifty minute time span, generating 82 pages of sites that were accessed on March 3, 2009, between 8:17 a.m. and 10:05 a.m. Examples noted in the investigation of site searches were for "erotic services." One site contained pornographic pictures of women and advertisements for erotic services. The investigation reviewed a two-week sample that was retrieved from Applicant's computer, indicating hundreds of "hits" to the erotic services site. It further noted that Applicant accessed the internet in the morning and continually clicked on different sites throughout the day until he left work. Applicant denied he had hundreds of "hits" but rather he thought it was less than a hundred, and more likely "in the tens."[5]

Applicant stated he left his internet on all day. He denied he spent any more time on the internet than 15 minutes every two-hour period. He did this four to five times a day. He stated that he spent the rest of the day reading. He believes the investigation is incorrect and that the 82-page list of "hits" is inaccurate. He thinks it is closer to 30 pages. His explanation is that there may have been automatic pop-ups on the computer. The investigation revealed that these sites were accessed through "search" questions. He does not know how his computer registered these entries. He denied he accessed a website about obtaining sex in Latin countries. He admitted he accessed Craigslist, but stated he was searching for a fish tank. He believes he was inadvertently diverted to the personal ads of the site. He admitted that on two to three occasions he went to the Craigslist website personal ads section, but he was reading the ads because he thought they were funny. He denied he intentionally accessed the site to view pornography, although it was on the website. He admitted he saw pornography on the website, but not all the time. His stated his access was accidental. His explanation for going back to a website that might be inappropriate was that if the site was not blocked by the information technology (IT) personnel at his place of employment, then it was permissible to access. He also explained he went back to the site because he did not have any work to do and his access was brief.[6]

Applicant explained that it is the company's IT personnel's job to block inappropriate websites. His asserted that if they did not block the website, he assumed it was appropriate to view regardless of content. He believed he has no personal responsibility or accountability for accessing a website that was not blocked.[7]

Applicant denied he was ever informed of his company internet policy regarding personal use. He denied he ever was provided a copy of the policy, read it, or was told

[5] Tr. 41-46, 111-113.

[6] Tr.23-28, 36, 41-45, 61-67, 72-73.

[7] Tr. 67, 73-76, 103-111, 115.

to review it. He did not ask about the policy. He understood that viewing pornography at work was inappropriate and there was a policy against viewing pornography and hate websites. He acknowledged being provided with the government client's internet policy.[8]

In March 2009, Applicant was suspended without pay during the investigation for accessing inappropriate internet sites and charging the U.S. Government for time worked while accessing the non-work related sites. He was terminated from his employment in April 2009 for his actions.

Applicant believed his privacy was violated by his company, when he learned they had researched the websites he was accessing from the internet on his work computer during working hours. He believed he should have been told that the company was monitoring his usage. He was upset that the company was "checking up" on him. He reiterated his position that the IT people should have prevented him from accessing inappropriate websites. He stated he believed he was not doing anything inappropriate because no one told him not to. He is upset that no one told him his internet use was a problem. Applicant never shared his password with anyone.[9]

In his interview with an Office of Personnel Management investigator, he explained that he was told by his supervisor that he was terminated from employment because he accessed the website Craigslist's personal section. When first questioned at this hearing, Applicant stated he did not know why he was terminated from his job. Later, he admitted he was told by his employer that he was terminated because of his inappropriate use of the internet.[10]

During the company's investigation, Applicant was provided a sample of the site listings retrieved from his account. He acknowledged to the investigator that he visited the sites. He also mentioned he had an addiction and he wanted to know if the company would give him an exception to using the internet. He believes he is addicted to the internet because his line of work is very tedious and complicated, and the internet refreshes and relaxes him. He acknowledged he had been to the Craigslist site. He was looking at classified ads and clicked on some and this is what led him to view inappropriate pictures. He told the investigator that since he got through, there must not be a problem accessing the site. He also suggested to the investigator that it was not his fault. He stated that if the IT group had made him aware that it was not an appropriate website, he would have stopped accessing the sites. He stated he needed the internet to do his job. At his previous employment, the pornographic sites were blocked. He told the investigator that he knew it was wrong, but did not think the

[8] Tr. 69-71, 97-99, 113-114; GE 2.

[9] Tr. 68, 103-111.

[10] Tr. 33-36, 55-57.

company was looking at [the] activity. He admitted to the investigator that he made a mistake when he went to the sites and it was "bad."[11]

When asked by the company's investigator how he charged his time when he was looking at these sites, he stated that he did not do anything different. He charged his time to whatever task he was assigned.[12]

Applicant's testimony throughout the hearing was not credible. He consistently lacked candor. His statements were repeatedly inconsistent. He did not understand that charging the government client when he was not doing work for them was inappropriate and likely illegal. His position was that if he did not charge the government client he would not get paid.

Applicant has not disclosed to his wife why he was terminated from employment with this company. His wife does not know he accessed inappropriate websites. He did not tell her because "I just look at those sites, I didn't do anything."[13] He acknowledged it would cause problems if he told his wife the truth about his termination. He stated he told his wife that the contract he was working on was finished and he was waiting for a new one. He did not disclose to his present employer why he was terminated from employment with his former employer.[14]

Applicant's mother and brother are citizens and residents of India. His mother was a teacher and retired about ten years ago. Applicant's father passed away in May 2010. His mother received an inheritance from his father. He was a retired college administrator. He did not receive a pension. She owns an apartment and Applicant's brother helps her financially. Applicant does not provide her financial support. His brother runs an information technology company. It is a private company and he has no government contacts. He is married and has two children. His wife does not work outside the home. Applicant's sister and brother-in-law both work for a college as instructors. They have one child.[15]

Applicant's in-laws are citizens and residents of India. His father-in-law is a retired bank general manager. The banks are all nationalized in India. He receives a pension. His mother-in-law is a home maker. Applicant and his wife do not provide financial support to her parents.[16]

[11] Tr. 61-70, 91-92, 102-111; GE 2.

[12] GE 2.

[13] Tr. 57.

[14] Tr. 52-61.

[15] Tr. 80, 89.

[16] Tr. 89-91.

Applicant traveled to India in 2010 to attend his father's funeral. He spent four weeks in India in 2009 and traveled there in 2004. He sees his family while there. His family is aware that he holds a security clearance. He owns no property or investments in India, but has a bank account that has about $8,000. He uses the account when he is in India and he receives a better foreign exchange rate. He has assets totaling approximately $650,000 in the United States.[17]

India[18]

India is a sovereign, socialist, secular, democratic republic. It is a multiparty, federal parliamentary democracy with a bicameral parliament and a population of approximately 1.1 billion.

The Indian government generally respects the rights of its citizens, but serious problems remain. Police and security forces have engaged in extrajudicial killings of persons in custody, disappearance, torture, and rape. The lack of accountability permeated the government and security forces, creating an atmosphere in which human rights violations went unpunished. A number of violent attacks were committed in recent yeas by separatist and terrorist groups. In November 2008, terrorists coordinated an attack at a hotel in Mumbai frequented by westerners.

The United States recognizes India as key to its strategic interests and has sought to strengthen its relationship with it. The two countries are the world's largest democracies, both committed to political freedom protected by representative government, and share common interests in the free flow of commerce, in fighting terrorism, and in creating a strategically stable Asia. However, differences over India's nuclear weapons program and pace of economic reform exist. There are also concerns about India's relations with Iran, including their increasing cooperation with the Iranian military.

There have been cases involving the illegal export, or attempted illegal export, of U.S. restricted, dual-use technology to India, including technology and equipment which were determined to present an unacceptable risk of diversion to programs for the development of weapons of mass destruction or their means of delivery. Foreign government and private entities, including intelligence organizations and security services, have capitalized on private-sector acquisitions of U.S. technology. In March 2008, an American businessman pleaded guilty to conspiring to illegally exporting technology to entities in India.

The United States views India as a growing world power with which it shares common strategic interests. There is a strong partnership between the two countries and they are expected to continue addressing differences and shaping a dynamic and collaborative future. The United States and India seek to elevate the strategic

[17] Tr. 82-86, 93-94.

[18] HE I.

partnership further to include cooperation in counter-terrorism, defense, education, and joint democracy promotion.

Policies

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 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, 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. 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, an "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 and has the ultimate burden of persuasion to obtaining a favorable clearance 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 safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation of 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

Guideline E, Personal Conduct

AG ¶ 15 expresses the security concern for personal conduct:

> 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. I have especially considered the following:

> (b) deliberately providing false or misleading information concerning relevant facts to an employer, investigator, security official, competent medical authority, or other official government representative.
>
> (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; 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 standings.

Applicant was suspended from work without pay for accessing inappropriate sites on the internet and charging the U.S. Government for time worked while accessing non-work related internet sites. This was in violation of his company's policies. He was later terminated from employment. Applicant deliberately provided false information to his employer when he denied accessing inappropriate websites. He has concealed the reason for his employment termination from his wife. I find these disqualifying conditions apply.

I have considered all the following mitigating conditions under AG ¶ 17 and the following three potentially apply:

(a) the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts;

(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; and

(e) the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress.

Applicant misused the internet, and charged a government client for work not done for over two months. Applicant refused to take responsibility for his wrongful actions. He did not comprehend that charging a client for work that was not done is wrong, unethical, and illegal. He did not take responsibility for intentionally accessing inappropriate internet sites. Rather, he blamed the IT personnel for allowing him to access such sites. He provided false information to his employer and did not correct his falsifications before being confronted with the facts. Applicant has concealed his employment termination from his wife. He failed to show positive steps he has taken to reduce or eliminate his vulnerability to exploitation, manipulation, or duress. I have considered all of the evidence and conclude none of the mitigating conditions apply.

Guideline B, Foreign Influence

AG ¶ 6 expresses the security concern regarding foreign influence:

Foreign contacts and interests may be a security concern if the individual has divided loyalties or foreign financial interests, may be manipulated or induced to help a foreign person, group, organization, or government in a way that is not in U.S. interests, or is vulnerable to pressure or coercion by any foreign interest. Adjudication under this Guideline can and should consider the identity of the foreign country in which the foreign contact or financial interest is located, including, but not limited to, such considerations as whether the foreign country is known to target United States citizens to obtain protected information and/or is associated with a risk of terrorism.

AG ¶ 7 describes conditions that could raise a security concern and may be disqualifying. The following are potentially applicable:

(a) contact with a foreign family member, business or professional associate, friend, or other person who is a citizen of or resident in a foreign country if that contact creates a heightened risk of foreign exploitation, inducement, manipulation, pressure, or coercion;

(b) connections to a foreign person, group, government, or country that create a potential conflict of interest between the individual's obligation to protect sensitive information or technology and the individual's desire to help a foreign person, group, or country by providing that information; and

(e) a substantial business, financial, or property interest in a foreign country, or in any foreign-owned or foreign operated business, which could subject the individual to heightened risk of foreign influence or exploitation.

Applicant's mother, parents-in-law, brother and sister are citizens and residents of India. Applicant maintains some contact with his family living there. His mother is self-sufficient, living off an inheritance. Applicant's brother may assist his mother. His brother is employed in private industry. His father-in-law receives a pension through a national bank, and his mother-in-law is a homemaker. Applicant visits India periodically. Applicant has some assets in India. His connections to family members in India could potentially create a heightened risk of foreign influence or potential conflict of interest. The above disqualifying conditions are raised.

I have also analyzed all of the facts and considered all of the mitigating conditions for this security concern under AG ¶ 8 and especially considered the following:

(a) the nature of the relationship with foreign persons, the country in which these persons are located, or the positions or activities of those persons in that country are such that it is unlikely the individual will be placed in a position of having to choose between the interests of a foreign individual, group, organization and interests of the U.S.;

(b) there is no conflict of interest, either because the individual's sense of loyalty or obligation to the foreign person, group, government, or country is so minimal, or the individual has such deep and longstanding relationships and loyalties in the U.S., that the individual can be expected to resolve any conflict of interests in favor of the U.S. interests;

(c) contact or communication with foreign citizens is so casual and infrequent that there is little likelihood that it could create a risk for foreign influence or exploitation; and

(f) the value or routine nature of the foreign business, financial, or property interests is such that they are unlikely to result in a conflict and could not be used effectively to influence, manipulate, or pressure the individual.

The mere possession of a close personal relationship with a person who is a citizen and resident of a foreign country is not, as a matter of law, disqualifying under Guideline B. However, depending on the facts and circumstances, this factor alone is sufficient to create the potential for foreign influence and could potentially result in the compromise of classified information. Applicant has family members who are citizens and residents of India. The United States maintains close relations with India. Applicant maintains some contact with his family and his wife's family in India. When he visits India he stays with his family. Based on the nature of his contacts, I cannot conclude that his relationship with his family is casual and infrequent. Therefore, I find AG ¶ 8(c) does not apply.

The nature of a nation's government, its relationship with the United States, and its human rights record are relevant in assessing the likelihood that Applicant's family members are vulnerable to government coercion. The risk of coercion, persuasion, or duress is significantly greater if the foreign country has an authoritarian government, a family member is associated with or dependent upon the government, the country is known to conduct intelligence operations against the United States, or there is a serious problem in the country with crime or terrorism. India has a close and friendly relationship with the United States. They are the two largest democracies in the world. Although India has had some human rights issues and some terrorist incidents, it does not appear that these involved exploiting their citizens. India is an active collector of U.S. economic intelligence. However, there is no indication that they target or exploit their own citizens to obtain it. It is also very unlikely that Applicant would be forced to choose between loyalty to the United States and his family in India. Based on India's relationship with the United States, it is very unlikely that intelligence officials would attempt to pressure Applicant's family to gather valuable or classified information from the U.S through Applicant. I find mitigating condition AG ¶ 8(a) applies.

All except Applicant's father-in-law, who is retired from working at a nationalize bank, have no known ties to the Indian government. I do not find Applicant's relationship with his family in India or his infrequent visits there create a heightened security risk. There is no evidence that India pressures its citizens to obtain classified information, and it is highly unlikely Applicant would have to choose between loyalty to his family in India and the United States.

Applicant has been an American citizen since 2003. His children are U.S. citizens, having been born here. His wife is also a U.S. citizen. Although he has relatives living in India, he also has his immediate family living in the United States. Almost all of his financial assets are located in the United States. He has minimal assets in India. His ties to the United States are significant. I find that Applicant is loyal to the United States and he can be expected to resolve any conflict of interest in favor it. Therefore, I find mitigating conditions AG ¶¶ 8(b) and (f) apply.

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 commonsense judgment based upon careful consideration of the guidelines and the whole-person concept.

I considered the potentially disqualifying and mitigating conditions in light of all the facts and circumstances surrounding this case. I have incorporated my comments under Guidelines E and B in my whole-person analysis. Some of the factors in AG ¶ 2 (a) were addressed under those guidelines, but some warrant additional comment. Applicant charged the U.S. Government for work he did not do. He failed to understand why his conduct is a security concern. He did not take responsibility for his actions when he accessed inappropriate websites on the internet. He did not grasp that his conduct was wrong and unethical. He was upset that his computer was being monitored by his company, which is how they learned of his conduct. Applicant's refusal to accept responsibility for his conduct raised a serious personal conduct security concerns involving his judgment. Applicant has not met his burden of persuasion on this issue. However, Applicant's contact with family in India is not security concern.

Overall, the record evidence leaves me with serious questions and doubts about Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude Applicant failed to mitigate the security concerns arising under the guideline for Personal Conduct. He has successfully mitigated the security concerns arising under the guideline for Foreign Influence.

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:	Against Applicant
Paragraph 2, Guideline B:	FOR APPLICANT
Subparagraphs: 2.a-2.c:	For Applicant

Conclusion

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

_____
Carol G. Ricciardello
Administrative Judge