DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 09-03693
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Kathryn MacKinnon, Esq., Department Counsel
For Applicant: Eric Eiser, Esq.

May 26, 2011

Decision

RICCIARDELLO, Carol G., Administrative Judge:

Applicant mitigated the Government's security concerns under Guidelines E, Personal Conduct, K, Handling Protected Information, and M, Use of information Technology Systems. Applicant's eligibility for a security clearance is granted.

Statement of the Case

On October 20, 2010, the Defense Office of Hearings and Appeals (DOHA) issued Applicant a Statement of Reasons (SOR) detailing security concerns under Guidelines E, K and M. 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 on November 18, 2010, and requested a hearing before an administrative judge. The case was assigned to me on April 5, 2011. DOHA issued a Notice of Hearing on April 13, 2011. I convened the hearing as scheduled on May 10, 2011. The Government offered exhibits (GE) 1 through 7. GE 1 through 3 and 5 through 7 were admitted into evidence without objection. Applicant objected to GE 4. The objection was overruled and GE 4 was admitted into evidence. Applicant offered exhibits (AE) A and B. They were admitted into evidence without objections. DOHA received the hearing transcript (Tr.) on May 16, 2011.

Procedural Matters

Department Counsel withdrew SOR allegation ¶ 1.d.

Findings of Fact

Applicant denied all of the SOR allegations except ¶¶ 1.e and 1.f. His admissions are included in the findings of facts. After a thorough and careful review of the pleadings, exhibits, and testimony, I make the following findings of fact.

Applicant is 48 years old. He married in 1996 and has one child. He is an engineer, and has worked for his current employer, a federal contractor, since 1999. He has a bachelor's and a master's degree. He holds a top secret security clearance.[1]

Applicant began working for Company A in approximately 1988. Company A was bought by Company B. Applicant continued his employment with Company B. While working for Company B, he transferred to a new site location. He packed up his belongings from his office, taking personal items and other work-related items, including documents and magnetic tapes that stored data, to assist him in his new assignment. Applicant did not review what was on the tapes. Classified, proprietary and sensitive items are distinctively marked. None of the items he packed were marked as classified, proprietary, or sensitive. In his job, he was not required to secure any of the material to which he had access. In 1992, Applicant ceased employment with Company B and packed his belongings, to include four or five boxes and approximately 20 pieces of magnetic media, and took them home.[2]

Applicant's former supervisor, when he worked at Company A, Witness X, testified on his behalf. He explained that when Applicant worked at Company A he had complete access to all of the company's information regarding the engineering systems. He carried a "beeper" and was trusted to access the company at all times. While working at Company A, Applicant did not violate any of the company's rules or policies. When he transferred sites, he was permitted to take the company's materials with him. The policy at the time was that all proprietary property was clearly labeled. He credibly testified that while he supervised Applicant, there was not proprietary or sensitive

[1] Tr. 91-93.

[2] Tr. 76-87.

information or property under his control or Applicant's. He explained that the proprietary information and documents that did exist, were not stored on computer disks or magnetic tapes, but rather were on drawings and within contract proposals. The magnetic tapes that existed were used as back-ups for data, and were locked in temperature-controlled rooms. Computer manuals and computer training manuals, were not proprietary or sensitive, and were available to the general public from the manufacturer. Witness X could not estimate the worth of the tapes and disks and did not know how the valued was determined. There is no evidence that any of the materials Applicant retained in the boxes were proprietary or sensitive.[3]

Witness X also provided a character letter in support of Applicant. In it he described Applicant "to be of excellent character, reliable, dependable, and trustworthy." He further noted:

> When employees elect to leave a company and move on, they clean out their cubicles, desk, filing cabinets, etc. During such a cleaning it is not uncommon for them to pack up listings of old code they've written, flow diagrams, etc., capturing as they do their own intellectual creations. I've never seen this as a violation of company policy; rather I see it as part of the normal course of a professional career.[4]

Applicant then began working for Company C in 1992. As part of a subcontract with Company C, Applicant worked directly for Company D. When his assignment with Company D was completed, he returned to Company C. He brought with him four separate computer programs in the form of paper print-outs that referenced the work he completed for Company D. He saved it in the event Company D had any questions or troubles, so he could answer them. He did not believe he took any proprietary or sensitive documents with him from Company D when he returned to Company C. He did not believe he was violating any rules or regulations, or that what he did was wrong. There is no evidence that any of these materials were proprietary or sensitive. He did not bring this material home, but rather it remained with Company C.[5]

From 1996 to 1998, Applicant worked for Company E. When he left his employment with Company E, he took with him approximately 50 diskettes. Except for two of the diskettes, the others were free diskettes received from America On-line (AOL) soliciting subscriptions to their service. Applicant had collected the AOL diskettes and erased the data on them and was going to use them for personal use at a later time. The two remaining diskettes contained information on projects Applicant had worked on. They included sample websites he developed for the company. The samples on the diskettes were a small part of information that was available to the public as "open

[3] Tr. 49-74.

[4] AE A.

[5] Tr. 102-109, 112, 177-178.

source" on the internet. None of the information was proprietary or sensitive. He provided the disks to government investigators during his background investigation. The disks were returned to him.[6]

As part of a background investigation for access to sensitive compartmented information (SCI), conducted by another government agency, Applicant was required to complete a polygraph examination. Applicant stated that the polygrapher believed he was withholding information. The polygrapher asked if there may have been something he took or did he steal something? Applicant credibly testified that he was only aware of things he took from his employers, so he speculated that perhaps contained in some of the disks there might be proprietary or sensitive information that may be causing the issue with the polygraph. He credibly testified that he was not aware that there actually was proprietary or sensitive information, but he was grasping at possibilities to appease the polygrapher. He had not looked at the disks or tapes that he had taken to see what was on them. Applicant was denied access to SCI by the government agency. He did not appeal the denial because he was working on a different project that did not require access to SCI.[7]

Regarding SOR 1.a, Applicant admitted he had four to five boxes and approximately 20 magnetic media at his home. When asked by the polygrapher what the value of it was, Applicant told him he did not know. The polygraph examiner continued to press him for a value so he guessed its value based on man-hours to develop the data on the medium, and then he guessed a dollar figure. He applied the same guesstimate formula when determining a dollar figure under the other allegations. He stated he used his best judgment to take items he believed he was authorized to take at the time.[8]

In August 2001, on three occasions, Applicant accessed a pornographic website on his employer's computer, after work hours. His supervisor confronted him and Applicant admitted he accessed the sites. It was against company policy, but Applicant stated he was unaware that it was prohibited because it was after hours. He was going through a difficult period with his wife, who had recently given birth to their son. He received a warning letter from his supervisor and there have been no other incidents. Applicant's wife is aware of the incidents.[9]

Applicant joined his current employer in 1999, and has been promoted to positions of increased responsibility, from a technical staff member, group supervisor for 40 employees, and now a project manager. He was responsible for ensuring all of his subordinates received proper security training. He prepared them for periodic security

[6] Tr. 118-133,163-166.

[7] Tr.87-95, 106-108, 114, 147-150, 174.

[8] Tr. 109-111, 176

[9] Tr. 133-137, 167-168, 175; GE 6, 7.

inspections. He was required to sign a nondisclosure agreement because of his access to proprietary information. He provided numerous letters from people he has worked for commenting on his excellent work ethic and expressing their gratitude for his accomplishments and devotion. He is recognized for his demonstrated technical leadership and managerial skills.[10]

Applicant has handled classified information in the past. He credibly testified that he ensured he complied with the proper procedures for transferring and handling classified data. A colleague provided a character letter for Applicant and detailed her first-hand knowledge of Applicant's adherence to security guidelines. In December 2008, Applicant was responsible for the coordination and delivery of classified laptop computers from his employer to the employer's sponsor. He met with the security officers to ensure all steps were properly executed and the required documents were completed. He ensured delivery and receipt was completed. He was applauded for the success of the delivery and receipt. In May 2009, he was again trusted with the transportation of classified laptops to a remote site to support a field test. Applicant was required to coordinate with his employer's security personnel and the recipient's security personnel to ensure proper procedures were followed. Through his tireless efforts, the transfer was successful.[11]

In 2010, Applicant's employer suffered a cyber attack that forced it to create new security policies. Applicant took the initiative to encrypt all of its program-critical files, in accordance with the policies, to prevent any future compromise. The company had multiple terabytes of data and itwas not a small undertaking. Applicant was "solely responsible for the program's security compliance and conducted it flawlessly."[12]

Applicant recently received an email with an attachment on an unclassified computer. He was concerned the attachment might be classified and immediately advised his supervisor of his concern. The computer was immediately locked down and a security review was conducted. It was determined the attachment was sensitive. The email and attachment were removed from the computer and from a smart phone device.[13]

During a walk-through of his spaces at work, Applicant noted an area that had been left unsecured with unmarked and marked classified documents. He followed proper protocol and shredded the documents. He determined who the responsible for leaving the area unsecured and discussed the issue with him. In addition, he advised the person's supervisor of the incident.[14]

[10] Tr. 137-147; AE B.

[11] Tr. 137-147; AE A

[12] AE A.

[13] *Id.*

[14] *Id.*

A witness who testified on behalf of Applicant has known him since 1985. After graduation from college they both worked for the same employer and shared an apartment. They worked together for two other companies. He described Applicant as a person with high integrity and a strong work ethic. He never had any performance problems, was easy to work with, and was respected by the staff. He noted:

> It should be noted that it is common practice for staff to leave a company with some sample work they may have developed such as software fragments provided that it is not proprietary or sensitive information and was retained simply as a basis for providing examples on practical development techniques to apply to future jobs. This is not unlike retaining software samples developed in school to apply on future academic and work activities.[15]

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 as to obtaining a favorable clearance decision."

[15] Tr. 37-46; AE A.

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 pertaining to 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 specifically considered the following:

> (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;
>
> (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. This includes

> but is not limited to considerations of: (1) untrustworthy or unreliable behavior to include breach of client confidentiality, release of proprietary information, unauthorized release of sensitive corporate or other government protected information. . . (3) a pattern of dishonesty or rule violations; (4) evidence of significant misuse of Government or other employer's time and resources; and
>
> (e) personal conduct, or concealment of information about one's conduct, that creates a vulnerability to exploitation, manipulation, or duress, such as (1) engaging in activities which, if known, may affect the person's personal, professional, or community standing.

I have considered the above disqualifying conditions and carefully considered all of the evidence presented. I conclude there is insufficient reliable evidence to conclude Applicant knowingly, deliberately, and without authorization removed proprietary or sensitive information and materials from his employer or while employed by different companies. There is insufficient evidence to conclude any materials he did remove from his employers were proprietary or sensitive. There is sufficient evidence to conclude he was counseled and received a disciplinary letter from his current employer for inappropriate use of the internet by accessing pornography on the job. I find AG ¶ 16(e) applies.

The guideline notes several conditions that could mitigate security concerns under AG ¶ 17. The following are potentially applicable:

> (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 viewed pornography on his company's computer on three occasions during a three-day-period in 2001. He was feeling alienated from his wife after the birth of their son. They have since resolved their difficulties. He admitted his behavior. He was counseled by his supervisor and the activity has not recurred. It has been ten years since the incident. It happened during an emotionally stressful time. Applicant's conduct occurred during a short period of time. I find AG ¶ 17(c) applies. Applicant's wife and employer are aware of the past behavior. He acknowledged the behavior, understands the seriousness of his actions, and has not repeated them. I find the behavior is unlikely

to recur. He was counseled by his employer. Because his wife and employer are aware of this past conduct, he is less vulnerable to exploitation, manipulation, or duress. I find AG ¶¶ 17(d) and 17(e) apply.

Guideline K, Handling Protected Information

AG ¶ 33 expresses the security concern pertaining to handling protected information:

> Deliberate or negligent failure to comply with rules and regulations for protecting classified or other sensitive information raises doubt about an individual's trustworthiness, judgment, reliability, or willingness and ability to safeguard such information, and is a serious security concern.

Guideline M, Use of Information Technology Systems

AG ¶ 39 expresses the security concern pertaining to use of information technology systems:

> Noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual's reliably and trustworthiness, calling into question the willingness or ability to properly protect sensitive systems, networks, and information. Information Technology Systems include all related computer hardware, software, firmware, and data used for the communication, transmission, processing, manipulation, storage, or protection of information.

After careful consideration of all of the evidence and analysis of the disqualifying conditions under AG ¶¶ 33 and 39, I conclude there is insufficient reliable evidence to conclude any of the disqualifying conditions under these guidelines apply. I will consider all of the evidence presented when analyzing the whole person.

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 K, M, and E in my whole-person analysis. Some of the factors in AG ¶ 2(a) were addressed under those guidelines, but some warrant additional comment. Applicant has been steadily employed since he graduated from college. He has a wife and a son. He has been consistently promoted and given increased levels of responsibility. In 2001, Applicant had a lapse in judgment when he viewed pornography after hours on his work computer. He was counseled and reprimanded, and there has not been a recurrence. Applicant admitted when he left employment he packed media items that he believed he was authorized to take and did not believe they had any proprietary or sensitive information on them. There was insufficient evidence to conclude that any of the items he had in his possession contained proprietary or sensitive material. I considered the character letters from Applicant's coworkers who cited specific instances where Applicant ensured all his employer's security procedures were followed and his dedicated efforts in practicing security awareness. I find Applicant has met his burden of persuasion. Overall, the record evidence does not leave me with questions or doubts about Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude Applicant mitigated the Personal Conduct, Handling Protected Information, and Use of Information Technology Systems security concerns.

Formal Findings

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

Paragraph 1, Guideline E:	FOR APPLICANT
Subparagraphs 1.a-1.c:	For Applicant
Subparagraph 1.d:	Withdrawn
Subparagraphs 1.e-1.f:	For Applicant
Paragraph 2, Guideline K:	FOR APPLICANT
Subparagraph 2.a:	For Applicant
Paragraph 3, Guideline M:	FOR APPLICANT
Subparagraph 3.a:	For Applicant

Conclusion

In light of all of the circumstances presented by the record in this case, it is clearly consistent with the national interest to grant Applicant a security clearance. Eligibility for access to classified information is granted.

_____
Carol G. Ricciardello
Administrative Judge