DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
----------	)	ISCR Case No. 08-02775
SSN: ----------	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Eric Borgstrom, Esq., Department Counsel
For Applicant: Warren J. Borish, Esq.

June 28, 2010

Decision

FOREMAN, LeRoy F., Administrative Judge:

This case involves security concerns raised under Guidelines E (Personal Conduct) and K (Handling Protected Information). Eligibility for access to classified information is granted.

Statement of the Case

Applicant submitted a security clearance application on April 27, 2007. On October 1, 2009, the Defense Office of Hearings and Appeals (DOHA) sent him a Statement of Reasons (SOR) detailing the basis for its preliminary decision to deny his application, citing security concerns under Guidelines E and K. DOHA acted 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 received the SOR on October 15, 2009; answered it on November 13, 2009; and requested a hearing before an administrative judge. DOHA received the request on November 18, 2009. Department Counsel was ready to proceed on January 31, 2010, and the case was assigned to me on February 5, 2010. DOHA issued a notice of hearing on March 2, 2010, scheduling the hearing for March 31, 2010. I convened the hearing as scheduled. Government Exhibits (GX) 1 through 10 were admitted in evidence without objection. Applicant testified, presented the testimony of four witnesses, and submitted Applicant's Exhibits (AX) A through G, which were admitted without objection. DOHA received the transcript (Tr.) on April 12, 2010.

Findings of Fact

In his answer to the SOR, Applicant admitted the allegations in SOR ¶ 1.d. He admitted some of the facts alleged in SOR ¶¶ 1.a-1.c, 1.e, 1.f, and 2.a-2.c but provided exculpatory explanations. I have treated his answers to SOR ¶¶ 1.a-1.c, 1.e, 1.f, and 2.a-2.c as denials. Applicant's admissions in his answer and at the hearing are incorporated in my findings of fact.

Applicant is a 48-year-old reliability engineer employed by a defense contractor. He received a bachelor's degree in electrical engineering technology in 1983 and a master's degree in reliability engineering in 1995. He has worked for his current employer since October 1985. He has held a security clearance since August 1988.

Applicant's supervisor, who has known him for about 25 years and supervised him for about 15 years, regards him as honest, ethical, and "absolutely law-abiding." He has "absolutely no doubts" about his suitability for a security clearance. (Tr. 91-92.) A coworker from 1985 to 1989 and a long-time friend testified that Applicant has a good reputation for honesty, integrity, and being a law-abiding citizen. (Tr. 103.) Another coworker for 21 years testified he is very honest. (Tr. 111.) A third coworker for 10 years testified he has a very good reputation for honesty and obeying the law. (Tr. 118.)

The allegations in SOR ¶¶ 1.a-1.c are based on another Government agency's report that Applicant admitted the conduct alleged in the SOR. The record does not include the other agency's report, nor does it include any documents from that agency reflecting the circumstances or content of Applicant's communication with that agency. The only evidence regarding the conduct alleged in the SOR was provided by Applicant in his answer to the SOR, his response to DOHA interrogatories (GX 4 and GX 5), a personal subject interview with an investigator from the Office of Personnel Management (GX 6), and his testimony at the hearing.

Applicant's parents emigrated from a foreign country and became U.S. citizens in the early 1960s. In July 1986, before Applicant was granted a clearance, his uncle and a diplomat from his parents' native country, with whom Applicant's uncle had served in the armed forces of that country, visited his parents' home. Applicant visited his parents on the way home from work and was introduced to the diplomat. The diplomat asked Applicant who he worked for and what he did. Applicant told him the name of his

employer, mentioned some unclassified program names, and explained the duties of a reliability engineer ("determine how long a piece of equipment will last before any kind of action is required to also ensure that the equipment is safe"). The diplomat did not probe for details. The conversation lasted about 15 minutes, and Applicant never had any further contact with the diplomat. Applicant disclosed this contact with a foreign diplomat during polygraph interviews with another agency in 1994 and in 1997. (GX 4 at 4-6; GX 6 at 3; Tr. 42-44.)

Although Applicant has held a clearance for most of the time he has worked for his current employer, he has worked on only one classified project that continued from 1994 to 1997. He did not work on any classified projects before 1994 or after 1997. (AX B; Tr. 29-33.) During his work on the classified project, he worked in an enclosed, secure area, and he was not allowed to remove any documents from that area. (Tr. 31-32.)

During security interviews with another agency in 1997, Applicant told an investigator that he routinely worked on "company confidential" materials at home. None of the materials were classified Confidential, Secret, or Top Secret by the Department of Defense. His employer has changed the term "company confidential" to "proprietary" to avoid confusion. (Answer to SOR at 1-2; GX 4 at 6, 9.)

Applicant worked at home for about two weeks on one project that was marked "For Official Use Only." He was directed by his supervisor to coordinate with a commercial graphics firm that was printing materials pertaining to the project. (Tr. 34-36.) Applicant testified that employees were encouraged to work at home to meet deadlines and that his employer had upgraded the office software so that engineers could work at home. (Tr. 38-39.) He admitted to the security investigator that he inadvertently left about 100 pages of "confidential" marked-up drafts of the graphics at home during the project. (Tr. 47.) He denied using the word "secret" in his security interview. He believed that the interviewer thought all working documents were classified because the interview took place at a location where everything was classified. (Tr. 63-64.)

Applicant testified that he believed that the limitations on use and distribution of proprietary information prohibited disclosure to competitors, but they did not preclude taking the material home, working on it at home, or traveling with it. (Tr. 62.) His supervisor testified that "casual overtime" using proprietary materials is encouraged, and that the company had spent "quite a bit of money" to provide secure software and facilitate working off-site. (Tr. 87-91.) Propriety information is required to be properly marked, but there is no requirement that it be stored in a locked container. (Tr. 94-96.)

In November 1990, Applicant was denied eligibility for access to sensitive compartmented information (SCI) by another agency. (GX 9; Answer to SOR, Attachments 1 and 2.) He asked for the basis of the denial and the responsible agency provided him with a "clearance decision summary" reflecting that he was interviewed by a security investigator "and was unable to successfully complete security processing."

The agency concluded that it was "unable to make an assessment of his ability to meet" the criteria for SCI access without his "full cooperation." (Answer to SOR, Attachment 6.) In May 1991, the agency determined that Applicant was eligible to reapply for SCI access if his employer sponsored him. (GX 10). He reapplied, with his employer's sponsorship, and he was granted SCI eligibility in May 1994. It was administratively terminated in April 2000 because he no longer needed it. (GX 8 at 3.)

Applicant testified that when he received the "clearance decision summary," he believed that his SCI application was disapproved because he had problems with the polygraph. He testified, "They kept telling me to relax when I was having the test, and I was like I was trying to relax, and they were yelling at me to relax, and one thing led to another and then that was the end." (Tr. 68.)

When Applicant submitted security clearance applications in September 2004 and April 2007, he answered "no" to the questions asking if he had ever had a clearance or access authorization denied, suspended or revoked. He did not disclose on either application that he had been denied SCI eligibility in November 1990. (GX 1 at Section 26b; GX 2 at Question 32.)

According to Applicant, when his SCI application was denied in 1990, his company security manager told him that the action on his SCI application was not a denial, and that he should not treat it as a denial because he was authorized to resubmit his application. (Tr. 55, 79.) The security manager informed him that no record of the decision on SCI access would be maintained in his employer's security file "or comparable government system." Applicant was advised "to only reveal the denial for access to SCI if [he] was specifically asked for any letters" regarding his security history. (GX 7 at 3.) On June 4, 2008, and September 12, 2008, Applicant provided copies of the documents pertaining to his SCI denial in response to DOHA interrogatories. (GX 5 at 6, 13-14; GX 7 at 4-9.)

Applicant's security manager retired in March 2002, but he provided a written sworn statement for the hearing, in which stated that he "may have advised" Applicant that his SCI access was not denied. (AX F.) Applicant's current special security officer submitted a statement supporting Applicant's recollection of the previous security manager's advice. (AX G.)

Policies

"[N]o one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988). As Commander in Chief, the President has the authority to "control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to have access to such information." *Id.* at 527. The President has authorized the Secretary of Defense or his designee to grant applicants eligibility for access to classified information "only upon a finding that it is clearly consistent with the national interest to do so." Exec. Or. 10865, *Safeguarding Classified Information within Industry* § 2 (Feb. 20, 1960), as amended and modified.

Eligibility for a security clearance is predicated upon the applicant meeting the criteria contained in the AG. These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, these guidelines are applied in conjunction with an evaluation of the whole person. An administrative judge's overarching adjudicative goal is a fair, impartial, and commonsense decision. An administrative judge must consider all available, reliable information about the person, past and present, favorable and unfavorable.

The Government reposes a high degree of trust and confidence in persons with access to classified information. This relationship transcends normal duty hours and endures throughout off-duty hours. 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 as to potential, rather than actual, risk of compromise of classified information.

Clearance decisions must be made "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." *See* Exec. Or. 10865 § 7. Thus, a decision to deny a security clearance is not necessarily a determination as to the loyalty of the applicant. It is merely an indication the applicant has not met the strict guidelines the President and the Secretary of Defense have established for issuing a clearance.

Initially, the Government must establish, by substantial evidence, conditions in the personal or professional history of the applicant that may disqualify the applicant from being eligible for access to classified information. The Government has the burden of establishing controverted facts alleged in the SOR. *See Egan*, 484 U.S. at 531. "Substantial evidence" is "more than a scintilla but less than a preponderance." *See v. Washington Metro. Area Transit Auth.*, 36 F.3d 375, 380 (4th Cir. 1994). The guidelines presume a nexus or rational connection between proven conduct under any of the criteria listed therein and an applicant's security suitability. *See* ISCR Case No. 92-1106 at 3, 1993 WL 545051 at *3 (App. Bd. Oct. 7, 1993).

Once the Government establishes a disqualifying condition by substantial evidence, the burden shifts to the applicant to rebut, explain, extenuate, or mitigate the facts. Directive ¶ E3.1.15. An applicant "has the ultimate burden of demonstrating that it is clearly consistent with the national interest to grant or continue his security clearance." ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002). "[S]ecurity clearance determinations should err, if they must, on the side of denials." *Egan*, 484 U.S. at 531; *see* AG ¶ 2(b).

Analysis

Guideline E, Personal Conduct

The SOR alleges that another Government agency reported that Applicant admitted removing classified information from his workplace for several years and

admitted discussing classified information with a non-U.S. citizen and family members (SOR 1.a). It also alleges that, from approximately 1985 through 1997, he removed classified material from his workplace (SOR ¶ 1.b), and that in the mid-1980's he discussed classified information with his mother, father, uncle, and a foreign diplomat (SOR ¶ 1.c). It further alleges that Applicant was denied SCI access by another agency in 1990 (SOR ¶ 1.d). Finally, it alleges that Applicant falsified his security clearance applications in 2004 and 2007 by intentionally failing to disclose that he was denied SCI access in 1990 (SOR ¶¶ 1.e and 1.f).

The conduct alleged in SOR ¶ 1.a is the same conduct alleged in SOR ¶¶ 1.b and 1.c. When the same conduct is alleged more than once under the same guideline, one of the duplicative allegations should be resolved in Applicant's favor. *See* ISCR Case No. 03-04704 (App. Bd. Sep. 21, 2005) at 3 (same debt alleged twice). Accordingly, I will resolve SOR ¶ 1.a in Applicant's favor.

The concern under this guideline is set out in AG ¶ 15 as follows:

> 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.

The evidence on which SOR ¶¶ 1.a-1.c was based was hearsay several times removed. It was provided by Applicant to an investigator, passed to an adjudicator, passed further to the other Government agency, and then finally passed to DOHA. While hearsay evidence is generally admissible in security clearance proceedings, the multiple levels of hearsay in this case significantly reduced the reliability of the information.

The allegation in SOR ¶ 1.b that Applicant removed classified materials from his workplace is based on his reported admission during a polygraph examination. The only evidence of the content of the polygraph interview was provided by Applicant. The evidence reflects that Applicant admitted removing "company confidential" information with the approval of his supervisor, and that the other agency's interviewer misunderstood his admission. His employer's security procedures made it virtually impossible to remove classified materials from the workplace. Applicant's reputation for honesty and law-abiding behavior make such a security violation highly unlikely. I found Applicant's account of the polygraph interview plausible and credible. I conclude that he has refuted the allegation in SOR ¶ 1.b.

The conversation with the foreign diplomat and Applicant's family members, alleged in SOR ¶ 1.c, occurred in July 1986, shortly after Applicant was hired and well before he had access to classified information. The only evidence in the record showing the nature of the information that was disclosed was provided by Applicant. The

information disclosed to the diplomat was generic and did not include classified, proprietary, or other protected information. I found Applicant's description of his conversation with the foreign diplomat plausible and credible. I conclude that he has refuted the allegation in SOR ¶ 1.c.

Applicant admitted the allegation in SOR ¶ 1.d, and his admission is corroborated by the documentary evidence in the record. The record reflects that the SCI denial was based on Applicant's failure to complete a polygraph examination and not on discovery of derogatory information. He was granted SCI eligibility in May 1994.

Security concerns arising from personal conduct may be mitigated if "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." AG ¶ 17(c). I conclude that the circumstances of the SCI denial, his subsequent receipt of SCI eligibility, and the passage of time since the denial are sufficient to mitigate security concerns raised by the SCI denial.

Applicant admitted his failure to disclose the other agency's denial of SCI eligibility on two security clearance applications, as alleged in SOR ¶¶ 1.e and 1.f, but he denied intentional falsification. When a falsification allegation is controverted, as in this case, the government has the burden of proving it. An omission, standing alone, does not prove falsification. An administrative judge must consider the record evidence as a whole to determine an applicant's state of mind at the time of the omission. *See* ISCR Case No. 03-09483 at 4 (App. Bd. Nov. 17, 2004). I conclude the evidence is sufficient to raise the disqualifying condition in AG ¶ 16(a) ("deliberate omission, concealment, or falsification of relevant facts from any personnel security questionnaire"), shifting the burden to him to rebut, explain, extenuate, or mitigate the facts. Directive ¶ E3.1.15. An applicant has the burden of proving a mitigating condition, and the burden of disproving it never shifts to the government. *See* ISCR Case No. 02-31154 at 5 (App. Bd. Sep. 22, 2005).

The relevant mitigating condition is AG ¶ 17(b):

> [T]he refusal or failure to cooperate, omission, or concealment was caused or significantly contributed to by improper or inadequate advice of authorized personnel or legal counsel advising or instructing the individual specifically concerning the security clearance process. Upon being made aware of the requirement to cooperate or provide the information, the individual cooperated fully and truthfully.

Applicant testified that he relied on the advice of his security manager. He provided the documents pertaining to his SCI denial in response to DOHA interrogatories. The security manager's advice and Applicant's explanation were plausible in light of the circumstances of the SCI denial, which arose from his inability or failure to complete a polygraph examination rather than the discovery of derogatory

evidence. Applicant's explanation was corroborated, albeit to a limited degree, by the statements from his former security manager and current security manager. I found Applicant to be sincere, candid, and credible at the hearing. I conclude that the mitigating condition in AG ¶ 17(b) is established.

Guideline K, Handling Protected Information

The SOR cross-alleges the conduct alleged in SOR ¶¶ 1.a-1.c under this guideline. The concern under this guideline is set out in AG ¶ 33 as follows: "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." The relevant disqualifying conditions are set out in AG ¶ 34 as follows:

> (a) deliberate or negligent disclosure of classified or other protected information to unauthorized persons, including but not limited to personal or business contacts, to the media, or to persons present at seminars, meetings, or conferences; and
>
> (b) collecting or storing classified or other protected information at home or in any other unauthorized location;

As noted above in the discussion of Guideline E, the allegation that Applicant disclosed classified information to family members and a foreign diplomat was refuted. Under Guideline K, disclosure of "other protected information" may raise a disqualifying condition. There is no evidence that Applicant disclosed "other protected information" to his family members or the foreign diplomat during their brief meeting in July 1986. There also is no evidence that Applicant's storage of protected but unclassified information at home violated any directives or company instructions. Thus, I conclude that no disqualifying conditions under this guideline are raised.

Whole-Person Concept

Under the whole-person concept, an administrative judge must evaluate an applicant's eligibility for a security clearance by considering the totality of the applicant's conduct and all the relevant circumstances. An 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 have incorporated my comments under Guidelines E and K in my whole-person analysis. Some of the factors in AG ¶ 2(a) were addressed under those guidelines, but some warrant additional comment.

Applicant is a mature, well-educated adult. He has worked for his employer for most of his adult life and held a clearance for many years. He was candid, sincere, articulate, and credible at the hearing. After weighing the disqualifying and mitigating conditions under Guidelines E and K, and evaluating all the evidence in the context of the whole person, I conclude Applicant has mitigated the security concerns based on personal conduct and handling protected information. Accordingly, I conclude he has carried his burden of showing that it is clearly consistent with the national interest to continue his eligibility for access to classified information.

Formal Findings

I make the following formal findings on the allegations in the SOR:

Paragraph 1, Guideline E:	FOR APPLICANT
Subparagraphs 1.a-1.f:	For Applicant
Paragraph 2, Guideline K:	FOR APPLICANT
Subparagraphs 2.a-2.c:	For Applicant

Conclusion

In light of all of the circumstances, it is clearly consistent with the national interest to continue Applicant's eligibility for a security clearance. Eligibility for access to classified information is granted.

LeRoy F. Foreman
Administrative Judge