DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 08-10088
SSN:	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Fahryn Hoffman, Esquire, Department Counsel
For Applicant: Gregory D. McCormack, Esquire

April 27, 2010

Decision

HOGAN, Erin C., Administrative Judge:

Applicant submitted a Questionnaire for Sensitive Positions on November 21, 2006. On October 29, 2009, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) detailing security concerns under Guideline E, Personal Conduct. 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 for SORs issued after September 1, 2006.

On November 23, 2009, Applicant answered the SOR and requested a hearing before an administrative judge. Department Counsel was ready to proceed on December 31, 2009. The case was assigned to me on January 12, 2010. The hearing was originally scheduled for February 11, 2010, but was cancelled due to inclement weather. On February 23, 2010, a Notice of Hearing was issued, rescheduling the hearing for March 17, 2010. The case was heard on that date. The government offered eight exhibits which were admitted as Government Exhibits (Gov) 1–8. Applicant testified and submitted no documents. The transcript (Tr.) was received on March 25,

2010. Based upon a review of the case file, pleadings, exhibits, and testimony, eligibility for access to classified information is denied.

Procedural Issues

During the hearing, Applicant presented evidence that another defense agency granted him eligibility for access to SCI on November 12, 2009. (Applicant's counsel mentioned he was granted a Top Secret/SCI clearance. The memo indicates Applicant was granted eligibility for SCI access. It is likely his Top Secret clearance was still valid. (s*ee* AE F)) This fact raised an issue of whether Applicant should be given reciprocity in accordance with section 2-204 of the National Industrial Security Program Operating Manual (NISPOM), dated February 28, 2006. Section 2-204 of the NISPOM states, in part:

> Any previously granted PCL that is based upon a current investigation of a scope that meets or exceeds that necessary for the clearance required shall provide the basis for a new clearance without further investigation or adjudication unless significant derogatory information that was not previously adjudicated becomes known to the granting agency.

I held the record open until March 31, 2010, to allow the parties to submit a response pertaining to the reciprocity issue. Both parties submitted a timely response. Department Counsel's response is marked as Hearing Exhibit (HE) I. Applicant's exhibit is marked as HE II.

Applicant contends that because another defense agency granted a personal clearance/access eligibility to the Applicant based upon a current investigation of a scope that met or exceeded that necessary for the clearance required Applicant should be issued a security clearance without the requirement of further investigation or adjudication. As a result, Applicant's counsel requests that the SOR be withdrawn. It is noted that Applicant's current supervisor provided a statement indicating a February 2008 incident report which concerns the allegations in SOR ¶¶ 1.d – 1.g was considered when adjudicating Applicant's SCI access which was granted on November 12, 2009.

Department Counsel contends that reciprocity does not apply because the SOR addresses matters that were not previously adjudicated, specifically, Applicant's job termination for cause in August 2009. Department Counsel admits that the other defense agency may have been aware of the February 2008 incident report when adjudicating his SCI access.

I find that reciprocity does not apply in Applicant's case because Applicant's termination for cause in August 2009 is additional derogatory information that was not considered when adjudicating Applicant's SCI access.

On another procedural issue, Department Counsel withdrew the allegation in SOR ¶ 1.c during the hearing. (Tr. 8)

Findings of Fact

In his Answer to the SOR, Applicant admitted the allegations in SOR ¶¶ 1.a, 1.b, 1.d, 1.g, and 1.h. He denied the allegations in ¶¶ 1.c, 1.e, and 1.f. During the hearing, Applicant changed his pleadings regarding to ¶¶ 1.e and 1.f from denials to admissions. (Tr. 71)

Applicant is a 31-year-old software engineer for a Department of Defense contractor who seeks to maintain his security clearance. He has been employed in his current position since November 2008. He enlisted in the United States Navy on August 28, 1997, and separated from active duty on October 20, 2005. He has held a security clearance since February 1998. He has a bachelor's degree in information technology and is currently studying for his master's degree. He is married and has three-year-old twin sons. (Tr. 28-35, 37, 75-77, 81; Gov 1; AE C)

In July 2005, Applicant received non-judicial punishment for violating Article 92, UCMJ, Failure to Obey a Lawful Order or General Regulation, and Article 128, UCMJ, Assault. His punishment included a reduction in rank from E-5 to E-4, 40 days restriction and extra duty, and forfeiture of $400 pay per month for two months. (Gov 5) The record does not go into detail pertaining to the facts that support the underlying offenses. Applicant testified that he was implicated in an investigation involving 25 other individuals related to selling orders for sex. He was not involved in the selling orders for sex offenses but was investigated for sexual harassment and fraternization charges. Although he was not an instructor, he apparently had asked out a female trainee and may have touched her on the shoulder. He denies that he was guilty of the offenses alleged in the NJP. (Tr. 31-33, 78-81; Gov 3 at 3-4)

On October 20, 2005, Applicant was involuntarily discharged from the United States Navy with a discharge characterized as general (under honorable conditions) discharge. The reason for the discharge was misconduct (serious offense). Applicant appeared before a discharge board before he was separated. (Gov 4; AE C)

When he separated from the Navy, Applicant worked for one employer for four months until he found employment with a large defense contractor (Company A) in March 2006. From March 2006 to November 2006, he worked at one location. In November 2006, he switched contracts and locations while still employed by Company A. (Tr. 86) In October 2007, Company A lost the contract, leaving Applicant without a job. At the time his sons were about a year old and his wife was not working. (Tr. 37, 40-42, 86; Gov 3 at 11)

After two weeks of unemployment, Applicant decided to list on his resume that he was a Certified Information System Security Professional (CISSP) in order to improve

his chances of being interviewed. Applicant was studying for his CISSP certification but did not have the certification when he listed it on his resume. He decided that he could list it on his resume and would have the certification by the time a prospective employer asked for proof. (Tr. 43, 88-89; Gov 3 at 11)

In September 2007, Applicant was interviewed and hired by Company B. During the interview, the program manager told him that it was great that he had his CISSP certification but it was not needed for a year. Instead of telling the program manager that he did not have the certification, Applicant said nothing because he thought it would give him more time to complete the certification. (Tr. 90-91; Gov 3 at 11) His program manager had a heart attack. The program manager who was in charge of the certification program for Company B replaced him. While on sick leave in late 2007, Applicant was sent an e-mail from the new program manager asking for his CISSP certification. Instead of telling the program manager that he did not have a CISSP certification, Applicant obtained a false certification document from a web-site that generated diplomas and certifications for a fee. He paid about $200 for the service. After he received the false CISSP certification, he sent it to the program manager. He testified that he knew he had crossed a line so he resigned the next day. This occurred in February 2008. (Tr. 46-50, 91-94; Gov 3 at 11-12)

Applicant states that this conduct was completely out of character for him. Being a new father and the only income-provider for his family contributed to his subsequent bad decisions. He does not intend to repeat similar conduct in the future. (Tr. 72-73, 119; Gov 3 at 12)

After he resigned from Company B, Applicant was unemployed for one and a half months. When he interviewed with Company C, he informed them about his false CISSP certification but was hired anyway. He later discovered that Company B sent in an incident report regarding the false CISSP certification related to his security clearance. In April 2008, he started to work for Company C. After about a month, Company C lost the contract and Applicant needed to find a new job. He worked as contractor for another government agency for a few months until he was hired back by Company A. He has worked for Company A since November 2008. (Tr. 52-59, 97-98)

In May 2009, Applicant was hired by Company D. This was a second full-time job. He was still employed full-time with Company A. He claims that his program manager at Company D was aware that he worked another full-time job. (It was actually his program manager at the work place who worked for the company who had the prime contract. Applicant's employer was a subcontractor.) On August 24, 2009, the Director of Human Resources from Company D notified Applicant that he was being terminated for inaccurate timekeeping. Applicant took time off to attend classes. Applicant believed that as long as he put his days off on the office calendar "it was okay." He certified his time cards before being paid twice a month. He did not list the time taken off to attend classes on his timesheets. At times, he would take days off and not indicate the days off on his timesheets. At the end of each pay period, he verified that the documentation

provided was true and accurate to the best of his knowledge. He also believed that his contract was not based on hours but on deliverables. (Tr. 60-67; Gov 6 at 2-3)

Company D's Director of Human Resources mentioned in an e-mail dated August 24, 2009, that she reminded Applicant that he had signed off on the company's timesheet policy and the acknowledgment of the company handbook which stated Company D's policies regarding total time accounting and timekeeping. (Gov 6 at 3-4) Applicant testified that he never received a copy of Company D's handbook or timesheet policy. He also never received ethics training. (Tr. 64-67, 99, 101-105)

Applicant testified that he believed that he was allowed paid time off to attend classes. He put the dates that he was at class on the public calendar and sent e-mails. He did not have a written agreement with Company D indicating that he could take paid time off to attend classes. He was told by the Human Resource Advisor that in government contracting you cannot claim for hours worked for a contract task unless you actually worked those hours. (Tr. 111-114; Gov 6 at 9)

The deputy project manager of the company that had the prime contract when Applicant worked for Company D wrote a letter stating that Applicant worked with him on a daily basis from 2008 to 2009. He describes Applicant as an "honest, hard working and dedicated individual." When he learned that Applicant was terminated for inaccurate timekeeping, he told his superiors that he believed there was a miscommunication. He believed the company that owned the prime contract and the government contractor approved Applicant's time away from the contract in order to attend classes. He states Applicant always let the Government and management know when he was not at work and taking classes. (I give the deputy project manager's assertions less weight because he did not testify and was not subject to cross examination.) The deputy project manager was also aware that Applicant was working a second job. He looks forward to working with Applicant on future projects. He believes that if Applicant is not granted a security clearance, it would be an unfortunate loss for the national interest of the United States. (AE A)

Company D had a policy that required employees to report outside employment to their immediate supervisor, group general manager, staff vice president, or ethics compliance officer. It would then be determined whether the outside employment would be permitted. Although Applicant told the deputy project manager that had the prime contract that he had another full-time job, it is unlikely he informed his superiors at Company D. I make this conclusion based on Company D's Human Resource Director's asking him on the day of his termination whether this was the first time he worked for a government contractor. (Gov 6 at 3; Gov 8; AE A)

Applicant's current government supervisor wrote a letter on Applicant's behalf. He is a retired Sergeant Major who served over 27 years in the U.S. Army. He states Applicant is a man of great integrity, who is dedicated to his family and work. He has known Applicant for two years and is impressed with his professional conduct. He

believes Applicant can be trusted and should be allowed to maintain his cleared status. The supervisor was aware of the February 2008 incident report when Applicant started to work for him two years ago. He claims Applicant was honest and wrote the necessary statements required by the government agency. He underwent an SCI background investigation and a government agency suitability determination. He indicates Applicant provides a positive influence and his truthfulness is an example for all to follow. (AE D, Letter of C.F., Sergeant Major, U.S. Army (RET), dated February 15, 2010)

Applicant provided additional character references. His references describe Applicant as "hard working," "conscientious," and "trustworthy." Most were informed of the SOR allegations and were surprised. (AE D) Applicant's performance evaluations while on active duty state that he meets or exceeds standards. His military awards and decorations include the Navy and Marine Corps Achievement Medal (2), Good Conduct Medal (2), National Defense Service Medal, Armed Forces Expeditionary Medal, Sea Service Deployment Ribbon, Navy Pistol Shot Ribbon (Marksman); and the Global War on Terrorism Service Medal. (AE C)

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 still required 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 as to obtaining a favorable security 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 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

Guideline E, Personal Conduct

The security concern relating to the guideline for Personal Conduct is set out in 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.

The following personal conduct disqualifying conditions potentially apply to the facts of this case:

> AG ¶ 16(a) (deliberate omission, concealment, or falsification of relevant facts from any personnel security questionnaire, personal history statement, or similar form used to conduct investigations, determine employment qualifications, award benefits or status, determine security clearance eligibility or trustworthiness, or award fiduciary responsibilities);
>
> 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);

AG ¶ 16(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 consideration 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; (2) disruptive, violent, or other inappropriate behavior in the workplace; (3) a pattern of dishonesty or rule violations; (4) evidence of significant misuse of Government or other employer's time or resources); and

AG ¶ 16(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).

AG ¶¶ 16(a) and 16(b) apply with respect to SOR ¶¶ 1.d, 1.e, and 1.f. Applicant knowingly provided false information on his resume in order to enhance his employment qualifications. During his job interview with Company B, he was given the opportunity to clarify that he was not CISSP certified but said nothing. When he was asked to provide proof of his CISSP certification, he purchased a false CISSP certification from a company based on the Internet. Applicant went to great lengths to falsely indicate that he was CISSP certified. He perpetuated the falsehood over the five-month period he was employed with Company B.

SOR ¶1.g is found for Applicant. This allegation does not raise a new pleading but rather summarizes facts that are relevant to the allegations in SOR ¶¶ 1.d, 1.e, and 1.f.

AG ¶ 16(d) applies pertaining to the allegations in SOR ¶¶ 1.a-1.e and 1.h. Between 2005 and August 2009, Applicant was involved in significant misconduct which raised issues of questionable judgment, untrustworthiness, unreliability, lack of candor, and willingness to comply with rules and regulations. In 2005, Applicant was punished under Article 15 for failure to obey orders and assault. While more information about the underlying offenses would have been helpful, it is clear that the Navy considered the offense was serious based on the subsequent involuntary discharge proceeding for misconduct (serious offense). From September 2007 to February 2008, he falsely claimed to be CISSP certified. He went to great lengths to perpetuate this falsehood. Sometime between May 2009 and August 24, 2009, Applicant inaccurately claimed that he worked hours on his timesheets when he was out of the office.

Although Applicant claims that he had permission to take paid time off from work at Company D when he was attending class, the management at Company D did not give him permission to do so. While the project manager of the company who held the primary contract wrote a letter stating Applicant let him know about his second job and about his time off, he was not an official representative of Applicant's company and did not have authority to grant approval. AG ¶ 16(d) applies because of Applicant's conduct between 2005 and August 2009 reveals a pattern of dishonesty and rule violations. His inaccurate timekeeping when employed at Company D raised additional questions about his integrity and is evidence of significant misuse of Government or other employer's time or resources. In Applicant's situation, it was a significant misuse of his employer's time and resources.

AG ¶ 16(e) applies because Applicant's past falsifications about his computer certifications made him vulnerable to exploitation, manipulation, or duress. Applicant was aware that if Company B discovered that he was not CISSP certified he would be fired. As a result, he took the falsehood one step further by purchasing a false certification over the Internet and presenting it to Company B. If Applicant were to be discovered, it would have affected his professional standing.

The following personal conduct mitigating conditions potentially apply to Applicant's case:

> AG ¶ 17(a) (the individual made prompt, good-faith efforts to correct the omission, concealment, of falsification before being confronted with the facts);
>
> 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); and
>
> AG ¶ 17(e) (the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress).

AG ¶ 17(a) does not apply. Applicant had the opportunity to tell the program manager during his interview with Company B that he did not have the CISSP certification. He chose not to say anything because he thought he would eventually become certified. He had another opportunity to say he was not certified when he was asked to provide a copy of his CISSP certification. Instead, he chose to purchase a false CISSP certification and present that to Company B. Although Applicant left his employment with Company B because he states he realized that he went too far, he never told Company B about the false certification document. Company B later filed an incident report in JPAS in February 2008. (This fact is not disputed although the record does not contain a copy of the incident report.) Although Applicant apparently disclosed the facts related to his falsely claiming that he was CISSP certified to his subsequent

employer, he did not disclose that he was not CISSP certified during the five months that he worked for Company B. Thus, he did not make a prompt good-faith effort to correct his deliberate falsification.

AG ¶ 17(c) does not apply because of the seriousness of Applicant's conduct. He has had a pattern of questionable behavior since 2005 when he received NJP for failure to obey an order and assault. An offense considered serious enough by the Navy to involuntarily discharge him for misconduct (serious offense). Two years later, he deliberately holds himself out as being CISSP qualified in order to enhance his job qualifications. Once hired, he perpetuates the falsehood for five months until he is told to provide his certification. He then obtains and presents a false CISSP certification rather than telling the truth. In May 2009, he is terminated for cause from Company D for inaccurate time-keeping. All of these offenses are serious. Applicant's behavior over the past five years raises questions about his judgment, trustworthiness and reliability.

AG ¶ 17(e) applies because Applicant subsequently disclosed the conduct related to his falsification of a CISSP certification to subsequent employers which reduced his vulnerability to exploitation, manipulation, or duress.

Overall, Applicant was involved in three significant incidents over the past five years that raise questions about his reliability, trustworthiness, and judgment. While he provided some mitigating evidence, each of these incidents raised questions about Applicant's integrity. Applicant has not mitigated the concerns under personal conduct.

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. While Applicant provided significant mitigating evidence, his history of questionable conduct over the past five years, the most recent incident occurring in August 2009, outweigh the mitigating evidence and raise questions about his ability to handle classified information. The security concerns raised under Personal Conduct are not mitigated.

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
Subparagraph 1.a:	Against Applicant
Subparagraph 1.b:	Against Applicant
Subparagraph 1.c:	Withdrawn
Subparagraph 1.d:	Against Applicant
Subparagraph 1.e:	Against Applicant
Subparagraph 1.f:	Against Applicant
Subparagraph 1.g:	For Applicant
Subparagraph 1.h:	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.

_____
ERIN C. HOGAN
Administrative Judge