DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 11-01583
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Richard Stevens, Esquire, Department Counsel
For Applicant: *Pro se*

10/04/2012

Decision

CREAN, Thomas M., Administrative Judge:

Based on a review of the pleadings, exhibits, and testimony, eligibility for access to classified information is denied.

Statement of the Case

On December 28, 2009, Applicant submitted an Electronic Questionnaire for Investigations Processing (e-QIP) to obtain a security clearance required for a position with a defense contractor. After an investigation conducted by the Office of Personnel Management (OPM), the Defense Office of Hearings and Appeals (DOHA) issued an interrogatory to Applicant to clarify or augment potentially disqualifying information in his background. After reviewing the results of the background investigation and Applicant's response to the interrogatory, DOHA could not make the preliminary affirmative findings required to issue a security clearance. DOHA issued a Statement of Reasons (SOR), dated May 25, 2012, detailing security concerns for handling protected information and personal conduct. These 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 in the Department of Defense on September 1, 2006. Applicant acknowledged receipt of the SOR on June 8, 2012.

Applicant answered the SOR on June 27, 2012. He admitted all allegations under both guidelines K and E. Department Counsel was ready to proceed on July 17, 2012. Applicant discussed the hearing date with Department Counsel on July 18, 2012, and the case was assigned to me on July 31, 2012. DOHA issued a Notice of Hearing on August 1, 2012, scheduling a hearing for August 16, 2012. I convened the hearing as scheduled. The Government offered three exhibits that I marked and admitted into the record without objection as Government Exhibits (Gov. Ex.) 1 through 3. Applicant testified. DOHA received the transcript of the hearing (Tr.) on August 29, 2012.

Findings of Fact

After a thorough review of the pleadings, transcript, and exhibits, I make the following essential findings of fact.

Applicant is 50 years old. He was born in Vietnam, and became a naturalized United States citizen in 1989. He received his bachelor's degree from a university in the United States in 1988. He has taken some postgraduate courses. He married his wife in 1988 but they divorced in 2006. He and his wife remarried in 2007. They have two children living at home. He was employed as an information systems administrator for a defense contractor from March 2009 until September 2010. (Tr. 14-15; Gov. Ex. 1, e-QIP, dated December 28, 2009)

Applicant commenced employment with a defense contractor as an information systems administrator in 2009. Starting in February 2010, he was receiving indoctrination and other training on the contractor's classified and unclassified systems. In March 2010, he was provided a classified user name and password for the classified system. Instead of memorizing this information, he wrote them in a word document and saved them in an unclassified system. He forgot about the document until he discovered it in July 2010. (SOR 1.b) He did not delete the document from his unclassified system. His company discovered the classified information on the unclassified system in August 2010 during a routine inventory of the unclassified system. (Tr. 20-21, 29-33; Gov. Ex. 2, OPM Investigation, dated November 12, 2010: Gov. Ex. 3, e-mails, dated August 30, 2010)

In March 2010, Applicant was working on the overnight third shift as an information systems administrator for the defense contractor. An employee put a classified hard drive on his desk for him to scan for viruses. The label identifying the hard drive as classified was on the bottom of the drive and not on the top. Applicant did not examine the drive to determine the classification of the drive. Applicant plugged the hard drive into an unclassified computer to scan for viruses. His supervisor saw the classified drive connected to the unclassified computer and directed Applicant to disconnect the drive (SOR 1.a). (Tr. 21, 27-29)

Applicant started work at the defense contractor's local office, but soon took a position at a different location. Applicant's family did not move to the new location so

Applicant had to drive nine hours one way a few times a month to visit them. When Applicant took this new position, he received a corporate credit card to use for his business expenses. He received written instruction that the card was to be used for business and not personal expenses, but he did not read the instructions. He used the card to purchase gas for his trips home as well as other personal items. He even used it to pay for some household items for his family. (SOR 2.a) The use of the credit card for personal items was a violation of company policy. After his company discovered that he was using the credit card for personal expenses, he was advised of the proper use of the company credit card. Applicant continued to use the company credit card for personal expenses. Applicant was not always home to get his mail and pay his bills, so he became delinquent in paying this credit card bill. The company learned of Applicant's continued unauthorized use of the credit card. He was involuntarily terminated from his employment for the unauthorized use of the credit card on September 28, 2010. (Tr. 21-22, 24-27; Gov. Ex. 3, e-Mails, dated August 30, 2012)

In November 2010, Applicant commenced employment as an information technology systems administrator with his present defense contractor employer. Applicant was interviewed on November 12, 2010, by an Office of Personnel Management (OPM) investigator concerning the application he submitted for a security clearance on December 28, 2009. By this time, Applicant had been terminated by the original defense contractor for cause, and was now working for another defense contractor. He told the investigator that he left employment with the original defense contractor for a better job. He had no issues or problems and left on good terms. In fact he had been terminated for cause. Applicant admitted lying to the investigator. (SOR 2.b; Tr. 22-24, 33-34; Gov. Ex. 2, Testimony, dated November 12, 2010) He stated:

> "So that was my mistake to tell the investigator that there was no problem at [defense contractor], that I actually had a letter of reprimand. I should have been honest and not tell her that. Because not to make an excuse about what I did, but I didn't want to lose my job, and nothing, no income to support—my wife was not working. And that was the only job I had in 2010. So I should have been honest and told her, yes, I was given a letter of reprimand because of the SIPERNET issue and the password, and got an involuntary termination. I should have told her that. Probably because I mentioned that I did not want to lose my job. I had to support my family, my wife and two small children." (Tr. 22-23)

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 must be considered in evaluating an applicant's eligibility for access to classified information.

These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, these guidelines are applied in conjunction with the factors listed in the adjudicative process. The administrative judge's overarching

adjudicative goal is a fair, impartial, and commonsense decision. According to AG ¶ 2(c), the entire process is a conscientious scrutiny of a number of variables known as the "whole-person concept." The administrative judge must consider all available, reliable information about the person, past and present, favorable and unfavorable, in making a decision.

The protection of the national security is the paramount consideration. AG ¶ 2(b) requires that "[a]ny doubt concerning personnel being considered for access to classified information will be resolved in favor of national security." In reaching this decision, I have drawn only those conclusions that are reasonable, logical, and based on the evidence contained in the record.

Under Directive ¶ E3.1.14, the Government must present evidence to establish controverted facts alleged in the SOR. Under Directive ¶ E3.1.15, the applicant is responsible for presenting "witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by applicant or proven by Department Counsel. . . . ." The applicant has the ultimate burden of persuasion in seeking 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 that 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.

Analysis

Handling Protected Information (Guideline K)

The deliberate or negligent failure to comply with rules and regulations for protecting classified or other sensitive information is a serious security concern. It raises doubt about an individual's trustworthiness, judgment, reliability, as well as a willingness and ability to safeguard such information. (AG 33)

Applicant made a copy of a classified user name and password and placed it into an unclassified system. He connected a classified hard drive to an unclassified computer. This information is sufficient to establish Handling of Protected Information Disqualifying Conditions AG ¶ 34(b) (collecting or storing classified or other protected information at home or in any unauthorized location; AG ¶ 34(c) (loading, drafting, editing, modifying, storing, transmitting, or otherwise handling classified reports, data, or other information on any unapproved equipment including but not limited to any typewriter, word processor, or computer hardware, software, drive, system, game board, handheld "palm" or pocket device or other adjunct equipment); and AG 34(g) (any failure to comply with rules for the protection of classified or other sensitive information).

I considered Handling of Protected Information Mitigating Conditions AG ¶ 35(a) (so much time has elapsed since the behavior, or it has happened so infrequently or under such unusual circumstances that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or good judgment); AG 35(b) (the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities; and AG 35(c) (the security violations were due to improper or inadequate training).

Applicant had two security violations in a short time, one in February 2010, and the other in March 2010. They occurred while he was in training to be a systems administrator for the classified system. There have been no other reported security violations. The security violations happened over two years ago in close proximity to each other. He was being trained at the time. Since the security violations happened while he was being trained, they are unlikely to recur. Since there have been no other violations, it appears he responded positively to his security training. Even though he discovered the user name and password in an unsecured word file in July 2010, it does not affect the mitigation of the security violation. Applicant mitigated the security violations for handling protected information.

Personal Conduct (Guideline E)

There is a security concern for conduct involving questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations, which 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 failure to cooperate with the security clearance process. A refusal to provide full, frank, and truthful answers to lawful questions of investigators, security officials, or other official representative in connection with personnel security or trustworthiness determinations will normally result in an unfavorable clearance action. (AG ¶ 15)

Applicant used his company-issued credit card for personal expenses in violation of company policy. It was the first time Applicant had been issued a company credit card. The e-mails between Applicant's supervisor and the human resource office (Gov. Ex. 3) show that after being advised of the rules for use of the credit card, Applicant continued to use it for personal expenses. Applicant was terminated by his employer for violation of the company credit card policy. When questioned about the reason for leaving this company, Applicant told the security investigator that he had no problems or issues with the employer and left on good terms for a better job opportunity. In response to the allegation in the SOR and at the hearing, Applicant admitted lying to the investigator about leaving the job on good terms. He stated he lied because he was concerned about losing his job since he was the only source of income for his wife and children. These facts raise Personal Conduct Disqualifying Conditions 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); and 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 regulation, or other characteristic indicating that the person may not properly safeguard protected information. This includes but is not limited to consideration of; (3) a pattern of dishonesty or rule violations; (4) evidence of significant misuse of Government or other employer's time or resources.

I considered all of the Personal Conduct Mitigating Conditions but particularly AG ¶ 17(a) (the individual made prompt, good-faith efforts to correct the omission, concealment, or 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(d) (the individual has acknowledged the behavior and obtained counseling to change the behavior or taken other positive steps to alleviate the stressors, circumstance, or factors that caused the untrustworthy, unreliable, or other inappropriate behavior, and such behavior is unlikely to recur. I find that these mitigating conditions do not apply. Applicant used his company-issued credit card for personal purchases in violation of company policy. Even after being advised of the violation, he continued to use the card for incorrect purchases. He deliberately lied to a security investigator about the termination from his former employer. He admitted the true facts only when confronted with the allegation in the SOR and at the hearing. The offense is not minor since it is a deliberate and direct false statement to a investigator in the process of a security investigation. It is recent in that it happened less than two years ago. Applicant admitted his gave a false statement for fear of losing his job and his income to support his family. He presented no information to indicate that he would not lie again in response to the same fears. While he has acknowledged his behavior, he presented no information to show he would not exhibit untrustworthy, unreliable, and inappropriate behavior again under the same circumstance. Applicant has not mitigated security concerns for personal conduct.

Whole-Person Analysis

Under the whole-person concept, the administrative judge must evaluate an applicant's security eligibility by considering the totality of the applicant's conduct and all 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 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. Applicant mitigated the security concerns for the two security violations when he was in training over two years ago. However, he did not mitigate the security concern for personal conduct. He continued to violate the company credit card policy after being advised of the violation. He deliberately lied to a security investigator concerning the reasons for his termination from a prior job. Applicant's personal conduct indicates that he may not be trustworthy, concerned, responsible, and careful regarding the safeguarding of classified information. Overall, the record evidence leaves me with questions and doubts as to Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude Applicant failed to mitigate security concerns for personal conduct. Access to classified information is denied.

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 K:	FOR APPLICANT
Subparagraphs 1.a and 1.b:	For Applicant
Paragraph 2, Guideline E:	AGAINST APPLICANT
Subparagraphs 2.a and 2.b:	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.

THOMAS M. CREAN
Administrative Judge