DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
----------	)	ISCR Case No. 07-04504
SSN: ----------	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Caroline H. Jeffreys, Esquire, Department Counsel
For Applicant: Philip B. Herron, Esquire

March 12, 2008

Decision

HOWE, Philip S., Administrative Judge:

Applicant submitted his Security Clearance Application (SF 86), on April 6, 2006. On September 28, 2007, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) detailing the security concerns under Guidelines K (Handling Protected Information) and E (Personal Conduct) for Applicant. 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 revised adjudicative guidelines (AG) promulgated by the President on December 29, 2005, and effective within the Department of Defense for SORs issued after September 1, 2006.

Applicant acknowledged receipt of the SOR on October 4, 2007. He answered the SOR in writing through counsel on October 12, 2007, and requested a hearing before an Administrative Judge. DOHA received the request on October 15, 2007. Department Counsel was prepared to proceed on November 30, 2007, and I received the case assignment on December 13, 2007. DOHA issued a Notice of Hearing on

December 18, 2007, and I convened the hearing as scheduled on January 9, 2008. The Government offered Exhibits (Ex.) 1 through 8, which were received without objection. Applicant testified on his own behalf and submitted Exhibits A and B, without objection. DOHA received the transcript of the hearing (Tr.) on January 25, 2008. Based upon a review of the case file, pleadings, exhibits, and testimony, eligibility for access to classified information is denied.

Findings of Fact

In his Answer to the SOR, dated October 15, 2007, Applicant admitted the factual allegations in ¶¶ 1.a. through 1.h. of the SOR, with explanations. He denied the factual allegations in ¶¶ 2.a. and 2.b. of the SOR. He also provided additional information to support his request for eligibility for a security clearance.

Applicant is 58 years old, married with three adult children, and is a retired military officer with 24 years of active service. He has a master's degree. Since his retirement in 1994, he has worked for several defense contractors. While in the military, Applicant had a security clearance and never had any incidents or problems with the clearance. During his career, Applicant completed several security clearance applications (SCS). A former supervisor evaluates Applicant as dependable and conscientious who always delivered a quality product for him. (Tr. 13-22, 49, 35, 55, 69, 80, 81; Exhibits 1 and A)

During a period of time from May 6, 2004, until February 27, 2006, Applicant perpetrated six incidents of failing to properly secure classified information in his work place. As a result of these incidents, no loss or compromise of classified information occurred. The safe, computer, and printer involved in the incidents were in a lockable room with a steel door and a swipe card mechanism, located amidst many work cubicles. After the incidents, he attended additional training regarding security procedures. The incidents were as follows:

(1) May 6, 2004, when Applicant printed a classified document and left it in the printer tray while he stepped outside the secured room to find a co-worker who needed to review the document. Another employee entered the secured room and found the classified document in the printer. Applicant was only gone a few minutes. At the end of the work day, Applicant closed the safe drawer, spun the combination lock dial, and pushed the handle to ensure it would not open. He signed the security checklist form and was the last person to do so that day.

(2) On May 7, 2004, another employee entered the secure room at the start of the work day and found the safe handle moved. She could open the safe by pressing on the drawer handle.

(3) On June 8, 2004, Applicant failed to secure the same safe. He spun the dial after closing the drawer, and pulled on the handle. Then he signed the security

checklist. The next morning, June 9, 2004, Applicant entered the secure room and found the safe drawer to be unlocked. He reported it.

(4) On July 13, 2004, the safe drawer was found to be unlocked by the person performing the end of day security checks. This person reported the safe appeared to be closed and locked, but was not locked. Applicant was the last person to access the area and the safe prior to the discovery of the unlocked safe. Applicant stated he remembered closing the drawer, spinning the dial, and signing the security checklist. He could not remember if he physically tugged on the drawer handle to determine if it were actually locked.

The safe was checked on September 27, 2004, and found to be working properly. The locksmith advised the defense contractor the dial must be fully spun and the handle depressed to make certain the safe is locked.

(5) On January 12, 2005, an employee performing the end of day security checks found the two drawer safe in the secure room unlocked. The safe opened when she pulled on the handle. Applicant was in the room previously that day to conduct his business. When completed, he closed the safe and spun the dial. When he should have pulled on the drawer handle, he noticed the printer was still on. He reached over to turn it off and check that no material, which should have been in the safe, was in the printer. Then he signed the security check list without testing the handle, and exited the room. About an hour later, the end of day security check showed the safe was unlocked.

(6) On February 27, 2006, Applicant was again in the secure room. After completing his work, he failed to remove the hard drive from a classified computer, and place it in the safe. He did lock the safe properly. (Tr. 33-37, 43, 50, 54; Exhibits 2-5)

Applicant's access to classified information was suspended on February 25, 2005, until restored on March 29, 2005. Applicant submitted a written response to the suspension. He stated he did not deliberately disregard procedures, and offered his version of the incidents up to the suspension. Applicant admitted he had no explanation for the security violations, but he thought he fully performed the security procedures. (Tr. 34, 54, 60; Exhibits 2, 4)

Applicant's employer removed him on April 12, 2006, at his work site after the sixth incident involving violations of security procedures. The employer found all prior incidents were of a similar nature. The employer found, "His repeated failure to comply with statutory requirements to protect classified information by following established processes and procedures is well documented." He was removed "to prevent future incidents and potential compromise of classified information." Applicant resigned from that job in May 2006. Applicant obtained employment with another defense contractor in a test evaluation position in May 2007. Applicant needs a security clearance to maintain that position. (Tr. 48, 62, 81; Exhibits 2, 5)

On August 20, 2007, Applicant offered a new explanation for his security lapses from 2004 to 2006. Applicant explained in this response to the DOHA interrogatories, and again at the hearing, that his younger sister died unexpectedly in February 2004. He was the estate executor, and had to spend three weeks working at her home to organize her possessions to settle the estate. Applicant's wife described him as tired during that period, and not sleeping well. Applicant described himself as numb over her death, but he had no breakdowns at work because he compartmentalized his life and focused on his work. He obtained no counseling during 2004, nor when his father-in-law was ill and died in the period of January to May 2006. Applicant considered his work performance from 2004 to 2006 to be high. Applicant had a physical examination in November 2007, and on December 31, 2007, evaluation by a clinical neuropsychologist. The tests results were normal. One test indicated some increasing stress, situational distress, and "some underlying depression and anxiety." No psychotherapeutic intervention was deemed warranted, "as the situational distresses have dissipated." (Tr. 25-32, 35, 50, 53, 63, 68-77; Exhibit B)

The National Industrial Security Program Operating Manual (NISPOM), dated January 1995 and as amended through 2004, DoD 5220-22-M, governs the security procedures pertaining to the storage and physical protection of classified information in the custody of contractors. It describes the types of safes to be used, and the security responsibilities for automated information systems. Applicant's actions violated Paragraphs 5-100, 5-300, 5-303, 8-100, and 8-105. (Exhibits 6-8)

Applicant completed his latest SCA on April 6, 2006. He started completing the form in February 2006. An employee of his employer physically wrote his answers into the last copy of the SCA. Applicant reviewed it and signed it. When he signed the SCA, he certified, as it states in the signature block, that "My statements on this form, and any attachments to it, are true, complete, and correct to the best of my knowledge and belief and are made in good faith. I understand that a knowing and willful false statement on this form can be punished by fine or imprisonment or both." Applicant answered Question 26(b), "To your knowledge, have you ever had a clearance or access authorization denied, suspended, or revoked, or have you ever been debarred from government employment?" Applicant answered "no" even though he had his access suspended from February 25, 2005, to March 29, 2005. He did not disclose the access suspension because he interpreted the question to apply only to his security clearance, which remained in effect. (Tr. 38-46, 55-61, 67; Exhibit 1)

Policies

When evaluating an Applicant's suitability for a security clearance, the administrative judge must consider the revised adjudicative guidelines (AG). In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially disqualifying conditions and mitigating conditions, which are useful 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, the administrative judge applies the guidelines in conjunction with the factors listed in the adjudicative process. The administrative judge's over-arching adjudicative goal is a fair, impartial and common sense 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, 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 K, Handling Protected Information

The security concern for Guideline K is set forth in AG ¶ 33 and states 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 guideline notes two disqualifying conditions that could raise security concerns under these facts: (1) AG ¶34(g), "any failure to comply with the rules for the protection of classified or other sensitive information," and, (2) AG ¶34(h), "negligence or lax security habits that persist despite counseling by management." The evidence of Applicant's six incidents of failing to lock the safe, remove classified information from a printer, and secure a classified hard drive in the safe shows these disqualifying conditions are clearly applicable. Applicant was retrained by management after the incidents. His access was suspended for a month in 2005, yet one more incident occurred in 2006. Then, management finally removed his access to classified information in 2006. Applicant could not credibly explain how the lapses in security procedures occurred. It was only in 2007 that he offered the reason that his grief over his sister's unexpected death may have caused him to forget to press on the safe handle as part of the locking procedure.

The guideline also includes three mitigating conditions that could be applicable here. Under AG ¶35(a), "so much time as 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," might be applicable on the passage of time element alone. Therefore, the latest incident was only two years ago, occurring after a suspension and several retraining sessions. The incidents did not happen infrequently, nor under unusual circumstances. The passage of time is insufficient to overcome the pattern of negligence exhibited by Applicant.

Nor are his present explanations for the incidents persuasive. It does not take much attention to duty and security requirements to spin a dial on a safe and pull on a safe handle at the end of a day to make certain the safe is locked. Repeatedly, Applicant could not do that. Finally, leaving a classified hard drive in a computer at the end of the work day is a more serious breach of security requirements. The mitigating condition does not overcome the two disqualifying conditions under these facts.

The other two possible mitigating conditions are not applicable. First, because Applicant did not respond favorably to his security retraining as shown by his subsequent failures to lock the safe. Second, as a well-trained military officer who had a clearance for 35 years and security training through out that time, there was certainly not any improper or inadequate training causing his several security failures.

Guideline E, Personal Conduct

The security concern under Guideline E is set forth in AG ¶15 and is stated 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 Government's concern here is two-fold. First, that the pattern of security breaches by Applicant in 2004 to 2006 demonstrate questionable judgment and an unwillingness to comply with rules and regulations that raise questions about Applicant's reliability, trustworthiness, and ability to protect classified information. Second, the Government is concerned about Applicant's failure to answer Question 26(b) truthfully when he denied he had ever had his access authorization denied, suspended or revoked.

The three disqualifying conditions under this guideline which apply are: ¶16(a), "involving 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, or determine trustworthiness," ¶16(c), "credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any 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 safeguard protected information," and ¶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 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."

Applicant committed each of the breaches of security regulations, responded to them as each was investigated by his employer, admitted he knew he had been suspended from access in 2005 for one month. He claimed his latest security violation was under investigation in April 2006 when he signed the SCA and that he had a security clearance at that time, but Question 26 was also clearly directed toward the access suspension occurring for one month in 2005. Applicant had a pattern of security

rule violations in 2004, 2005, and 2006. These disqualifying conditions clearly meet the facts and circumstances of Applicant's actions.

The mitigating conditions under this guideline are several, all involving efforts made by any Applicant to acknowledge and correct their behavior. Examining each of them, I concluded that none apply to Applicant under the facts of this case.

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) 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. Applicant is a mature and well-educated retired military officer, who for some unknown reasons could not lock a safe containing classified information on repeated occasions. These failures are serious errors in the requirements to protect classified information. His behavior did not change over a two-year period. His employer finally revoked his access in 2006 because it could no longer trust him to comply with the security requirements. Based on the evidence of his actions, the employer's action was prudent because there is a likelihood of continuation or recurrence of such security breaches.

Overall, the record evidence leaves me with questions or doubts as to Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude Applicant did not mitigate the security concerns arising from his conduct in handling of protected information, and his failure to disclose to the Government on his 2006 SCA his access suspension in 2005. Therefore, I conclude the Guideline K, Guideline E, and "whole person" concept against Applicant.

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:	AGAINST APPLICANT
Subparagraph 1.a:	Against Applicant
Subparagraph 1.b:	Against Applicant
Subparagraph 1.c:	Against Applicant
Subparagraph 1.d:	Against Applicant
Subparagraph 1.e:	Against Applicant
Subparagraph 1.f:	Against Applicant
Subparagraph 1.g:	Against Applicant
Subparagraph 1.h:	Against Applicant
Paragraph 2, Guideline E:	AGAINST APPLICANT
Subparagraph 2.a:	Against Applicant
Subparagraph 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 national security to grant Applicant eligibility for a security clearance. Eligibility for access to classified information is denied.

PHILIP S. HOWE
Administrative Judge