DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 03-08257
SSN:	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Emilio Jaksetic, Esquire, Department Counsel
For Applicant: Robert D. L'Heureux, Esquire

January 31, 2008

Remand Decision

ANTHONY, Joan Caton, Administrative Judge:

Applicant's noncompliance with security regulations in 1999 and 2000 raised doubts about his trustworthiness and ability to safeguard classified information. At his hearing on remand, Applicant produced credible refutation and mitigation for five of six alleged Guideline K security violations. However, his personal conduct, when reviewed in light of a whole person analysis, raised security concerns which he failed to mitigate. Clearance is denied.

The Defense Office of Hearings and Appeals (DOHA) declined to grant or continue a security clearance for Applicant. On March 23, 2005, under the applicable Executive Order[1] and Department of Defense Directive,[2] DOHA issued a Statement of Reasons (SOR), detailing the basis for its decision–security concerns raised under Guideline K (Security Violations) and Guideline E (Personal Conduct) of the Directive.

[1]Exec. Or. 10865, *Safeguarding Classified Information within Industry* (Feb. 20, 1960), as amended and modified.

[2]Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (Jan. 2, 1992), as amended and modified.

On April 11, 2005, Applicant submitted an answer to the SOR and elected to have a hearing before an administrative judge. The case was assigned to me November 22, 2005. On February 24, 2006, I convened a hearing to consider whether it was clearly consistent with the national interest to grant or continue a security clearance for Applicant. I continued Applicant's hearing, and it resumed on March 8, 2006. The Government called no witnesses, introduced 13 exhibits (Ex.), and offered one document for administrative notice.

Applicant, who appeared *pro se*, objected to each of the Government's proposed exhibits. His objections were overruled. Applicant called no witnesses. Three of Applicant's proposed exhibits, D, F, and G, were e-mails composed and transmitted when Applicant was employed by a previous government contractor. Applicant was unable to affirm that matters referred to in the e-mails were not classified. I did not admit Applicant's Ex. D, F, and G. I returned the three exhibits to him, advised him to consult with an attorney or his security manager about the documents in question, and continued the hearing.

When his hearing resumed on March 8, 2006, Applicant again appeared *pro se* and attempted to introduce four additional e-mail documents and was unable to affirm that the documents did not contain or allude to classified information.[3] I returned the documents to Applicant, and did not admit them to the record.

Applicant introduced 10 documents which were not admitted into evidence. He withdrew one proposed exhibit before it was identified. The following exhibits introduced by Applicant were admitted into evidence: Ex. A, C, I, J, K, L1 through L-8, M, N, O, P, Q, R, S, T, U, and V. DOHA received the transcript (Tr. I) of the February 24, 2006 proceeding on March 6, 2006; it received the transcript (Tr. II) of the March 8, 2006 proceeding on March 16, 2006.

On June 12, 2006, I issued a decision denying Applicant's security clearance. Applicant appealed. On February 8, 2007, DOHA's Appeal Board found it could not conclude from the record that Applicant had received the due process provided for in Executive Order 10865 and the Directive, and it remanded the case and directed me to reopen the case and provide Applicant with a new hearing. The Appeal Board pointed out that it was error for me to fail to preserve a complete record for appeal by returning to Applicant the exhibits he had offered and which I had not admitted into evidence. Further, the Appeal Board noted:

> Where a document is offered as an exhibit by one of the parties and discussed on the record, the document (or a copy thereof) should be marked for identification by the Judge and placed in the file of the case, even if the Judge concludes that the document should not be admitted into evidence. [Citations omitted.] Department of Defense rules should be applied to documents that are classified or are

[3] None of the documents offered by Applicant contained markings indicating they were classified documents.

> reasonably suspected of being in need of classification review.

ISCR Case NO. 03-08257 at 5 (App. Bd. Feb. 8, 2007.)

To comply with the Appeal Board's directions, I convened a new hearing for Applicant on May 16, 2007. The hearing convened on May 16, 2007, and produced a transcript of 469 pages. The Government called no witnesses and introduced 14 Exhibits (Ex.), which were marked as Government's Ex. 2-1 through 2-14. The Government also introduced one document for administrative notice, which was marked as Ex. 2-15. Applicant objected to the admission of Government Ex. 2-9 and Ex. 2-10. I admitted the two exhibits over Applicant's objections. I noted that the two exhibits contained adverse e-mail communications, composed in 2000, from Applicant's workplace. I advised the parties that I would carefully assess how much weight I would give to each exhibit. Government Exs. 1 through 8 and 11 through 14 were admitted to the record without objection. Government Ex. 15 was also admitted without objection.

Applicant testified on his own behalf and called five witnesses. In addition, Applicant introduced 24 Exhibits, which were marked Applicant's Ex. A-2-1 through A-2-24. Applicant's exhibits were admitted to the record without objection. Applicant's Ex. A-2-16 was an e-mail communication from a former co-worker of Applicant's. At the conclusion of the hearing, I left the record open so that Applicant could submit a letter from the co-worker in lieu of the e-mail. On May 23, 2007, Applicant submitted, by facsimile, the letter from the co-worker and asked that it be entered in the record as a substitute for the e-mail previously entered as Ex. A-2-16. Department Counsel did not object to Applicant's request. Accordingly, Applicant's new Ex. A-2-16 was entered in the record of the proceeding. DOHA received the transcript of the proceeding on May 30, 2007.

Findings of Fact

Based on the entire record in this case, including Applicant's hearings of February 24, 2006, March 8, 2006, and May 16, 2007, all exhibits entered into evidence, and the testimony of Applicant and all witnesses called, I make the following findings of fact:

The SOR in this case contains eight allegations of disqualifying conduct under Guideline K, Security Violations, and four allegations under Guideline E, Personal Conduct. In his answer to the SOR, Applicant admitted eleven of the twelve allegations but denied they were disqualifying conduct under Guidelines K and E. He denied that four allegations he admitted under Guideline K were security concerns under Guideline E. He noted mitigating circumstances. Applicant's admissions are incorporated as findings of fact.

Applicant is 49 years old. Since 2005, he has been employed as a senior systems scientist by a government contractor. He holds a bachelor of science degree in electronics and engineering and a master of science degree in mechanical and

aerospace engineering. He is taking course work toward a Ph.D degree. He has held a security clearance since 1983. (Tr. I, 12; Tr. III at 207, Ex. 1; Ex. C.)

Applicant was married in 1982 and divorced in 1986. He is the father of two adult children. (Ex. 1.) He has not remarried. In 1988, Applicant was incarcerated for three days by order of a state circuit court judge following a complaint by his ex-wife that Applicant was harassing her. On the security clearance application (SF-86) he certified on February 10, 2006, Applicant supplied information about his ex-wife and then added the following additional comment: "Not an individual that I would recommend for a position of trust. . . ." (Ex. 2-1, Ex. 2-14.)

From July 1986 to March 1987, Applicant was employed by a government contractor (Employer A) as a systems analyst. Between about February 6, 1987 and March 4, 1987, Applicant was orally counseled or was issued deficiency/misconduct notices approximately seven times. The counseling and deficiency notices related to tardiness, poor work performance, failure to follow company procedures in working with support staff, failure to meet production deadlines, and unprofessional demeanor. (Ex. 2-13.)

When Applicant worked for Employer A, he sought to organize a company-sponsored volleyball team; in cooperation with Applicant, the company's human resources department provided him with a roster of employees who wanted to play on the company's team. The county where the team sought registration required that all volleyball players certify with their signatures that they were residents of the county. When Applicant obtained the list, there were several prospective players who had not signed to verify their status as county residents. Without their permission, Applicant signed the names of those employees on the roster. He then caused the roster to be filed with the county. Thereafter, he sought reimbursement from the employer of the filing fees he paid to the county to register the roster of players. Employer A fired Applicant on approximately March 9, 1987 for violating its business practices and ethics. Applicant filed a claim for unemployment benefits form his state of residence after he was fired. The state unemployment commission hearing examiner found that the nature of Applicant's separation from his employment disqualified him from receiving unemployment benefits. Applicant appealed. On appeal, the state employment commission found that Applicant's employer set forth a prima facie case of misconduct and that the record supported a finding that Applicant "was discharged for unethical conduct concerning his efforts to organize an employer/sponsored volleyball team." (Ex. 2-11 at 3-5, Ex. 2-12; Tr. III, 340-348.)

Applicant objected to the inclusion of the information about his falsification of the co-workers' signatures because it occurred 18 years ago. He testified that he thought off-duty conduct had some relation to on-duty conduct, but he characterized his on-duty conduct as "sterling" and he asserted the employer did not specify how he had violated the business practices and ethics code. (Ex. N; Tr. II, 107.) DOHA alleged in SOR ¶ 2.c. that Applicant's conduct in falsifying the signatures of his co-workers raised a security concern under Guideline E.

Applicant certified an application for federal employment (SF-171) on August 23, 1989. Question 39 on the SF-171 asks an applicant for federal employment if he or she has been fired from any job in the previous ten years. Applicant responded "yes" to Question 39 and reported his firing from Employer A as "act[ing] inappropriately in forming a company-sponsored sports team" and being accused by his employer "of forging signatures for the roster." He then added: "I believe the true reason for the termination was due to my inability to control my then ex-wife and her harassment of me at my place of work." At his hearing on remand on May 16, 2007, Applicant opined that he was fired from his job by Employer A because the company mangers failed to appreciate his work and found his engineering assessments "did not go along with their geopolitical goal as a company." (Ex.2-2 at 3, 12; Tr. III, 348-350.)

On the SF-171 he completed on August 23, 1989, Applicant reported he worked as a project task leader for Employer B from January 1989 to April 1989. He reported, also in response to Question 39, that he left Employer B under threat of termination. He also reported that Employer B alleged he had violated his contract and withheld his last paycheck. (Ex. 2-2 at 3-4.)

From 1996 to 2005, Applicant was employed by a government contractor as an electrical engineer (Employer C). He left that job under unfavorable circumstances. On the SF-86 he certified on February 10, 2006, Applicant stated he left his job as an electrical engineer as the result of "change in employer requirements. Employer felt I was unable to fill any other jobs that they had at that time." (SF-86, signed by Applicant on February 10, 2006, at 26.) At his hearing on March 8, 2006, Applicant explained he left his job as an electrical engineer because an individual who reviewed his work did not think he performed his job adequately. (Tr. II, 103-104.)

In his work as a government contractor, Applicant was responsible for the protection of classified information. During the period 1999 to 2000, he did not have original or derivative classification authority. He had recommended classification authority. He relied on agency guidance for a determination of what was and was not classified information. (Tr. III, 368-372.)

In March 1999, as a part of his regular duties, Applicant received a spreadsheet, and it was his job to gather and compile unclassified information to go on the spreadsheet format. Once this was done, Applicant passed the spreadsheet to another individual, who posted the spreadsheet on an unclassified web site. In November 1999, Applicant was responsible for updating the information on the spreadsheet. After he updated the unclassified information by e-mail, officials in another office, who had received the e-mail, informed his chain of command that a certain part of the spreadsheet contained information that was classified. Applicant's supervisors did not agree the information was classified, but they eventually acceded to the designation proposed by the other office. They removed the specified information from the spreadsheet and the website, and it was labeled classified. The military manager who was responsible for providing Applicant with the spreadsheet information provided a statement for the record, which reads, in pertinent part, as follows: "The information was not deemed classified . . . when posted on the web or during the updating of the spreadsheet; it became classified upon the subsequent ops-coordinated review.

[Applicant] had no way of knowing the information was classified." (Ex. A-2-16; Ex. 2-8; Tr. III, 241-248.) In SOR ¶¶ 1.a. and 1.b., DOHA alleged that Applicant was responsible for security incidents arising from the information posted on the spreadsheet in March 1999 and November 1999.

On February 29, 2000, Applicant's security manager sent an e-mail notification to the chief military officer in Applicant's chain of command notifying her that when Applicant had closed the unit's office the previous evening, he had failed to initial the outside form or to initial that he had performed the closing checklist.[4] Applicant stated his employer did not inform him of this incident. On April 7, 2000 and April 9, 2000, Applicant was responsible for securing his work facility. On April 7, 2000, he failed to properly secure the combination lock and to perform other steps to activate motor sensors in the office. On April 9, 2000, he also failed to secure the combination lock and to pull a small pin attached to a lock on the door. Later, security inspectors found the unsecured deadbolt locks. Applicant learned the procedure for closing the office by watching his co-workers perform the task. He had not received formal training. He did not learn about pulling the pin on the lock until April 10, 2000. Because Applicant's conduct was in violation of paragraphs 5-102 and 5-103 of the NISPOM, he was decertified to open and close the secure work area by himself after the incidents of April 7 and 9, 2000, until he had received further training.[5] He did not receive further training while assigned to that command, and he did not request further training from the command. These three security incidents were alleged at SOR ¶¶ 1.c., 1.d., and 2.b. (Tr. III, 292-300, 336-340, 385-390; 422-423, Ex. 2-4, Ex. 2-9, Ex. 2-15.)

On May 9, 2000, a major, identified as a security manager, observed Applicant at a meeting and sent an e-mail to a senior officer in Applicant's chain of command expressing concern about Applicant's handling of classified information.[6] The security manager stated that during the meeting, Applicant began to copy an unclassified file from a classified laptop computer to move it to an unclassified projection computer, without using secure copy. The security manager concluded that if Applicant had not been stopped, the projection computer would have become classified. In addition, the security manager observed that Applicant was using an unmarked disk to store the files for the briefing and that he left the briefing room with out securing the classified laptop., Applicant's failure to follow these required security procedures was alleged at ¶¶ 1. e(1), 1.e(2), and 1.e(3) of the SOR. The allegations raised security concerns under ¶¶ 4-102 (c), 8-102(c), 4-200, 1-200, 5-100, and 5-200 of the NISPOM. (Tr. II, 72-74; Tr. III, 302-321, 392-403; Ex. 10; Ex. 2-10, Ex. 2-15.)

---

[4]The government alleged this fact in SOR 2.b. To corroborate the allegation, the government provided at Ex. 2-4 at 4, a photocopied document identified as "Security Container Check Sheet" marked "Mar 00." It was not possible to decipher whether an entry was or was not made on February 28, 2000.

[5]The decision to decertify Applicant was made by a colonel who was chief of the division on the basis of information supplied to him by the major identified as the unit's security manager. (Ex. 2-4.)

[6]Ex. 2-8 identifies the author of the e-mails in Ex. 2-9 and Ex. 2-10 as the "[Deleted] security manager." In testimony on remand, Applicant identified the individual as " 1 of 30 officers that I dealt with and actually wasn't one of the more significant ones, so I can't say it was a security issue and he brought it to my attention." (Tr. III at 403.)

At his hearing on remand, Applicant stated the security manager's allegations were not brought to his attention. He disputed the conclusion that plugging a classified computer into a projector would have caused the projector to become classified. He observed that an unclassified disk put into an unclassified computer would not classify the computer. He stated that it was unlikely that a disk would have been brought into the briefing since the laptop computer used for the briefing was already loaded with the information to be used at the briefing. He also clarified the chain of responsibility for handling classified computers in his office (Tr. III, 302-320.)

In July 2000, Applicant attended a quadrennial defense briefing. Two military officers managed the briefing. Applicant attended the briefing as a representative of his work unit. Some of the material discussed at the briefing was classified. At the conclusion of the meeting, Applicant wrote a summary of the matters discussed at the meeting. Because he had attended many similar briefings, he felt confident he could distinguish between the classified and non-classified material discussed at the meeting. He sent the summary he had written to the two military officers who had conducted the meeting and asked them to confirm that his summary was accurate. One of the officers responded on a collateral matter within 24 hours, and Applicant interpreted his response as a confirmation that his summary was accurate. He did not hear immediately from the second officer. Acting on his interpretation that the first officer thought his summary was accurate, Applicant sent his summary by e-mail on an unclassified network to about 20 people in his office. Soon after the e-mail was sent, it was determined that Applicant's summary contained classified information, and the classified information had been sent over an unclassified system. Applicant was removed from his job and reassigned the next day to another office and another project. An investigation was conducted . Applicant's conduct was categorized as a security deviation which resulted in no damage to national security. (Ex. 2-5; Tr.III, 321-333, 403-406, 416-421.) This security violation was alleged at ¶ 1.f. of the SOR and identified as a violation of paragraph 5-403 of the NISPOM.

DOHA alleged that the security incidents alleged in ¶¶ 1.a., 1.b., 1.c., 1.d., and 1.e. of the SOR revealed questionable judgment, unreliability, and unwillingness to comply with rules and regulations, conduct that created a security concern under Guideline E of the Directive. (The SOR at ¶ 2.a. alleges the Guideline K disqualifying conduct is also disqualifying conduct under Guideline E.) Applicant did not deny the conduct, but he denied it was a security concern under Guideline E. (Answer to SOR.)

Applicant submitted a letter of character reference from his first-line supervisor, who had worked with him for approximately six months. The supervisor praised Applicant's honesty, integrity, and technical skill. (Ex. L-1.) Applicant supplied additional e-mail transmissions and letters of character reference from present and former co-workers, all of whom attested to his trustworthiness. (Ex. L-2 to L-8.; Ex. I, Q, .R, S, T, U.) He also supplied letters of appreciation he received from managers who evaluated his work in 1991 and 1997. (Ex. J; Ex. M.) At his hearing on remand, Applicant called five witnesses. Four of the witnesses had worked directly with the Applicant, and they testified to his care in handling classified information. All four witnesses also testified that they had not seen the SOR and were not aware of the allegations in Applicant's case. (Tr. 97-99, 104, 114-117, 126-127, 137-140, 145-146, 157-161, 170.)

I take administrative notice of the following sections of the National Security Program Operating Manual (NISPOM), DoD 5220.22-M, dated January 1995: ¶¶ 5-403, 5-102, 5-103, 4-102(c), 8–102(c), 4-200, 1-200, 5-100, 5-200.

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 occupy a position . . . that will give that person access to such information." *Id.* at 527. The President has restricted eligibility for access to classified information to United States citizens "whose personal and professional history affirmatively indicates loyalty to the United States, strength of character, trustworthiness, honesty, reliability, discretion, and sound judgment, as well as freedom from conflicting allegiances and potential for coercion, and willingness and ability to abide by regulations governing the use, handling, and protection of classified information." Exec. Or. 12968, *Access to Classified Information* § 3.1(b) (Aug. 4, 1995). Eligibility for a security clearance is predicated upon the applicant meeting the security guidelines contained in the Directive.

Enclosure 2 of the Directive sets forth personal security guidelines, as well as the disqualifying conditions (DC) and mitigating conditions (MC) under each guideline. In evaluating the security worthiness of an applicant, the administrative judge must also assess the adjudicative process factors listed in ¶ 6.3 of the Directive. The decision to deny an individual a security clearance is not necessarily a determination as to the loyalty of the applicant. *See* Exec. Or. 10865 § 7. It is merely an indication that 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 disqualify, or may disqualify, the applicant from being eligible for access to classified information. *See Egan*, 484 U.S. at 531. The Directive presumes a nexus or rational connection between proven conduct under any of the disqualifying conditions listed in the guidelines and an applicant's security suitability. *See* ISCR Case No. 95-0611 at 2 (App. Bd. May 2, 1996).

Once the Government establishes a disqualifying condition by substantial evidence, the burden shifts to the applicant to rebut, explain, extenuate, or mitigate the facts. ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002); *see* 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.

Analysis

Guideline K - Security Violations

In the SOR, DOHA alleged under Guideline K of the Directive that Applicant failed to comply with security regulations on six occasions. DOHA further alleged that Applicant's non-compliance resulted in eight security incidents which violated nine provisions of the NISPOM. (*See* NISPOM ¶¶ 1-200, 4-102(c), 4-200, 5-100, 5-102, 5-103, 5-200, 5-403, and 8-102(c).) In his answer to the SOR, Applicant admitted the eight security incidents specified in the SOR at ¶¶ 1.a. through 1.f. Noncompliance with security regulations raises doubt about an individual's trustworthiness, willingness, and ability to safeguard classified information. E2.A11.1.1.

Under the adjudicative Guideline K applicable in this case, security concerns are raised and could be disqualifying when there is an unauthorized disclosure of classified information (E2.A11.1.2.1) and when an applicant is responsible for violations that are deliberate or multiple or due to negligence. (E2.A11.1.2.2.)

Applicant's everyday work conditions as a government contractor required using and protecting classified information. Because they identify possible unauthorized and deliberate or negligent disclosures of classified information, SOR allegations 1.a., 1.b., and 1.f. raise security concerns under Disqualifying Condition (DC) E2.A11.1.2.1 and DC E2.A11.1.2.2. At his hearing on remand, Applicant provided credible information establishing that he placed unclassified information on a spreadsheet that was later transmitted to an unclassified web site in March 1999. He also provided credible information that the same information was not classified when he updated the spreadsheet in November 1999 and e-mailed it via an unclassified web site to others authorized to receive it. He also provided credible information to establish that some of the information on the spreadsheet was later upgraded to classified as the result of an internal review. Accordingly, I conclude that Applicant rebutted SOR allegations 1.a. and 1.b. and demonstrated that his actions as alleged in SOR ¶¶ 1.a. and 1.b. were not in violation of paragraph 5-403 of the NISPOM.

SOR allegation 1.f. also raises security concerns under DC E2.A11.1.2.1. and DC E2.A11.1.2.2. At his remand hearing, Applicant testified that in July 2000, he wrote a summary of matters discussed at a quadrennial defense briefing and felt confident that his summary did not contain classified information. He sent his summary to the two military officers who were responsible for the meeting. He heard back from one officer, and he interpreted the officer's response as clearance to send his summary as an unclassified document. Applicant sent his summary as an unclassified e-mail document over an unclassified network. The e-mail summary was reviewed and determined to contain classified information. Applicant was removed from his position and assigned to another office and another project. An investigation was conducted and Applicant's conduct was deemed to be a security deviation which resulted in no damage to national security.

Applicant's actions resulted in the unauthorized disclosure of classified information. While his unauthorized disclosure of classified information was not

deliberate, it appears to have been caused by negligence consequent to misplaced confidence in his ability to distinguish classified and unclassified information. Applicant possessed neither original nor derivative classification authority. In creating his summary he had a duty to request clarification regarding the information in the summary and whether it was classified or unclassified. He failed to exercise that duty but relied on assumptions that his past methods of inquiry for clarification were sufficient to prevent the unauthorized disclosure of classified information in this instance. His assumption that one of the two officers had provided clearance for the release of his summary was not correct.

We turn to an examination of applicable mitigating conditions under Guideline K. An applicant may mitigate security violation concerns if he shows the security violations were inadvertent ¶ E2.A11.1.3.1; isolated or infrequent ¶ E2.A11.1.3.2.;due to improper or inadequate training ¶ E2.A11.1.3.3.; or if the individual demonstrates a positive attitude toward the discharge of security responsibilities ¶ E2.A11.1.3.4.

Applicant's security violation appears to have occurred not through inadvertence but through a failure to exercise the due care required of a person entrusted with the responsibility for working with and protecting classified information. (*See* NISPOM, 1-200, 5-100, and 5-200.) His violation was not isolated or infrequent, but occurred within a context of inattentiveness that suggests a habit or pattern of behavior. Accordingly, mitigating conditions E2.A11.1.3.1 and E2.A11.1.3.2 do not apply to Applicant's case.

I also conclude that the security violation alleged at SOR 1.f. did not occur as the result of improper or inadequate training, and, therefore, mitigating condition E2.A11.1.3.3 is inapplicable.

Applicant is a highly trained engineer whose livelihood is premised on work requiring him to protect classified documents and information. Four of Applicant's witnesses testified to his present carefulness in protecting classified information. None of the witnesses was aware of Applicant's previous security incidents. Applicant defended his previous conduct that led to the security incident alleged at SOR 1.f., thus making it difficult to ascertain whether he had developed a specific plan for avoiding future security violations. Accordingly, I conclude that mitigating condition E2.A11.1.3.4. applies only in part.

SOR allegations 1.c. and 1.d. specify two incidents, one on April 7, 2000 and one on April 9, 2000, when Applicant failed to close his office by properly securing a combination lock and performing other steps to activate motor sensors in the office. When he attempted to close the office on April 9, 2000, he also failed to secure the combination lock and to set a small pin attached to the lock on the door. Applicant's failure to lock up his secure facility was reported to his security manager. After these incidents were reported, Applicant was decertified to open and close the secure work area by himself until he received remedial training. His command did not provide the remedial training, nor did Applicant request it.

At his remand hearing, Applicant testified credibly that, prior to the security incidents, he had never received formal training in locking up his secure facility, and he

had learned to lock up by watching other employees carry out the task. He acknowledged he didn't know about setting the pin on the lock.

Applicant's failure on two occasions to lock up his work facility securely raises a security concern under DC E2.A11.1.2.2. I conclude that this conduct was inadvertent and due to improper or inadequate training. Accordingly, mitigating conditions E2.A11.1.3.1 and E2.A11.1.3.3. apply.

On May 9, 2000, Applicant's security manager sent an e-mail to a senior military official describing his concern about Applicant's handling of classified information. The contents of this e-mail constitute SOR allegations 1.e(1), 1.e(2), and 1.e(3). Allegation 1.e(1) states that Applicant started to copy an unclassified computer file from a classified laptop to an unclassified projection computer without using secure copy. Allegation 1.e(2) states that Applicant used an unmarked disk to store files for the briefing. Allegation 1.e(3) states that Applicant failed to secure a classified laptop computer at the end of the meeting.

The record is silent regarding the response of the senior official to the security manager's e-mail allegations. Nothing in the record suggests that the allegations in the security manager's e-mail were investigated or brought to Applicant's attention at the time they allegedly occurred. Nothing in the record corroborates the allegations in the security manager's e-mail. I conclude the evidence has very little weight in establishing that Applicant is responsible for the security violations alleged. Additionally, Applicant provided credible testimony refuting the allegations. Accordingly, I conclude SOR allegations 1.e(1), 1.e(2), and 1.e(3) for Applicant.

Guideline E - Personal Conduct

In the SOR, DOHA alleged that the Guideline K security incidents alleged at ¶¶ 1.a., 1.b., 1.c., 1.d., and 1.e. constituted security concerns under Guideline E of the Directive (¶ 2.a.); that on February 29, 2000, when Applicant closed the office, he failed to initial the security checklist to show it had been carried out, and he did not initial the outside form in the proper location (¶ 2.b.); that in March 1987, he was fired for misconduct for violating his employer's code of business practices and ethics by falsifying the signatures of individuals on a roster for a company-sponsored volleyball team in order to obtain reimbursement for expenses relating to registering the team (¶ 3.c.); and that from February 6, 1987 to March 4, 1987 he was either orally counseled or given written employee deficiency/misconduct notices for being late for work, being late on projects, producing poor quality work, or for having an unprofessional attitude. (¶ 4.d.)

Guideline E conduct raises security concerns because it involves questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations and could indicate that an applicant may not properly safeguard classified information. Directive ¶ E2.A5.l.l.

In his answer to the SOR, Applicant denied allegation 2(a) because he had already addressed the allegations enumerated there as security violations under ¶¶

1.a. through 1.e. He admitted allegation 2(b) but denied it was of security significance under Guideline E. He also admitted allegations 2(c) and 2(d).

Allegation 2(b) states that Applicant failed to follow required procedures for closing his office by initialing a security checklist on February 29, 2000. The government's evidence in support of allegation 2(b) is barely legible and fails to corroborate the allegation. I conclude allegation 2(b) for Applicant.

Allegation 2(a) enumerates the security violations alleged at SOR 1(a), 1(b), 1(c), 1(d) and 1(e) and alleges that those facts raise personal conduct concerns about Applicant's judgment and unwillingness to comply with rules and regulations. Allegations 2(c) and 2(d) allege personal conduct that raises concerns about Applicant's judgment, trustworthiness, reliability, and willingness to comply with rules and regulations. Applicant's conduct raises security concerns under Guideline E Disqualifying Conditions (DC) E2.A5.1.2.1. and DC E2.A5.1.2.4.[7] Applicant's personal conduct in failing to acknowledge the conduct that led to his firing from Company A increases his vulnerability to coercion, exploitation, or duress.

We turn to an examination of possible Mitigating Conditions (MC) under the Guideline. Because Applicant's former employer and associates provided information about his unprofessional conduct that was substantiated and pertinent to a determination of his judgment, trustworthiness, or reliability, MC E2.A5.1.3.1 is inapplicable.

The conduct alleged in ¶ 2(a) occurred in 1999 and 2000, but it demonstrated an on-going pattern of inattentiveness and failure to follow rules and regulations for protecting classified information. The conduct alleged in ¶¶ 2(c) and 2(d) occurred almost 20 years ago, in 1987. However, in his hearings, Applicant continued to justify his conduct in 1987 and did not appear to understand why his employer fired him for falsifying a roster by signing the names of individuals who did not meet the residency requirement of the county in which the company-sponsored team would play. Further, Applicant presented the falsified roster to his employer for reimbursement of filing fees. Applicant offered two other reasons for his firing. In 1989, two years after he was fired, he opined that he was fired because his ex-wife was harassing him at work. In 2007, at his hearing on remand, he speculated that the company managers fired him in 1987 because his engineering assessments "did not go along with [the company's] geopolitical goal as a company." Applicant's attempts to justify his actions that gave rise to his termination from Company A suggest that he has not taken positive steps to come to terms with his conduct, a situation that continues to make him vulnerable to coercion, exploitation, or duress. Accordingly, I conclude that MC E2.A5.1.2.4. is not applicable.

[7]DC E2.A5.1.2.1 reads: "Reliable, unfavorable information provided by associates, employers, coworkers, neighbors, and other acquaintances." DC E2.A5.1.2.4. reads: "Personal conduct or concealment of information that increases an individual's vulnerability to coercion, exploitation or duress, such as engaging in activities which, if known, may affect the person's professional, or community standing or render the person susceptible to blackmail."

Whole Person Analysis

In addition to evaluating the disqualifying and mitigating conditions under each guideline, an administrative judge must thoroughly consider and review of all available reliable information about the appellant, past and present, favorable and unfavorable, to arrive at a balanced decision. Enclosure 2, ¶ E2.2.1 of the Adjudicative Guidelines describes this process of scrutiny and evaluation as "the whole person concept." The factors to be considered in a whole person analysis include the nature, extent, and seriousness of the conduct; the circumstances surrounding the conduct, to include knowledgeable participation; the frequency and recency of the conduct; the individual's age and maturity at the time of the conduct; the voluntariness of participation; the presence or absence of rehabilitation and other pertinent behavioral changes; the motivation for the conduct; the potential for pressure, coercion, exploitation, or duress; and the likelihood for continuation or recurrence.

Applicant completed a SF-171 in August 1989. He completed a SF-86 in December 1998 and another SF-86 in February 2006. These documents reveal that Applicant had a contentious relationship with his ex-wife and was incarcerated for three days in 1988 for harassing her. Eighteen years later, in 2006, when he completed his SF-86, he added a line stating that he would not recommend his former wife for a position of trust, an observation that seemed beside the point when added to his security clearance application. Applicant's documents also show he was fired from jobs or left under threat of termination in 1987 (Employer A), 1989 (Employer B), and 2005 (Employer C). Applicant provided several different reasons for his job terminations, suggesting he had not assessed or come to terms with the conduct that led to the terminations. He explained that his firings occurred because his work was not appreciated or because individuals who reviewed his work did not think he performed his job adequately. He also speculated he was fired by Employer A in 1987 because his wife was harassing him at work. He did not appear to accept the determination that Employer A fired him for an ethics violation, even when the state unemployment commission denied him benefits after finding he had been fired for violating his employer's code of business and ethical conduct.

Applicant's personal conduct that led to the allegations of security violations suggests a pattern of inattention to rules and procedures. His lack of attention to the details of protecting classified information caused him to take actions that raised security concerns under Guideline K. His present defense of his past unwillingness to comply with rules and regulations raises security concerns under Guideline E.

In ISCR Case No. 98-0761 at 3 (Dec. 27, 1999), DOHA's Appeal Board states that an administrative judge, in deciding an applicant's security worthiness, "must consider the record as a whole (Directive Section F.3.) and decide whether the favorable evidence outweighs the unfavorable evidence, or *vice versa*." I have considered the record as a whole and have evaluated Applicant's conduct under the whole person concept of the Directive. I conclude that the favorable evidence does not outweigh the unfavorable evidence and that Applicant has not demonstrated that it is clearly consistent with the national interest to grant him a security clearance.

Formal Findings

The following are my conclusions as to each allegation in the SOR:

Paragraph 1. Guideline K: AGAINST APPLICANT

Subparagraph 1.a.:	For Applicant
Subparagraph 1.b.:	For Applicant
Subparagraph 1.c.:	For Applicant
Subparagraph 1.d.:	For Applicant
Subparagraph 1.e(1):	For Applicant
Subparagraph 1.e(2):	For Applicant
Subparagraph 1.e(3):	For Applicant
Subparagraph 1.f.:	Against Applicant
Paragraph 2. Guideline E:	Against Applicant
Subparagraph 2.(a):	Against Applicant
Subparagraph 2.(b):	For Applicant
Subparagraph 2.(c):	Against Applicant
Subparagraph 2.(d):	Against Applicant

Decision

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 or continue a security clearance for Applicant. Clearance is denied.

Joan Caton Anthony
Administrative Judge