DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 07-06380
	)	
Applicant for Security Clearance	)	

Appearances

For Government: David F. Hayes, Esq., Department Counsel
For Applicant: David P. Price, Esq.

September 14, 2011

Decision

MENDEZ, Francisco, Administrative Judge:

Applicant mitigated the Guideline K concern. The minor, inadvertent security violations at issue here were a result of Applicant's workload, the lax security culture that his employer previously fostered, and sharing office space with others who, at times, willingly violated the security rules knowing Applicant would be held responsible. None of the violations resulted in the compromise of classified information, and the last security incident occurred over three years ago. Applicant has since changed the behavior and attitude that led to the violations, and has become a role model in the handling of protected information. Clearance is granted.

Statement of the Case

Applicant has held a security clearance since 1973 and been employed by the North Atlantic Treaty Organization (NATO) since 1999. He submitted a security clearance application (SCA) in September 2006. He was subsequently interviewed by and provided an affidavit to a government investigator as part of his background investigation in June 2008. He then responded to a Defense Office of Hearings and Appeals (DOHA) interrogatory in September 2009.

Based upon the adverse information Applicant provided in his 2008 affidavit and 2009 interrogatory response, DOHA made a preliminary decision to deny him access to classified information on January 11, 2010. The basis for this decision is set forth in a Statement of Reasons (SOR), which alleges the security concern of Guideline K (Handling Protected Information).[1] Applicant responded to the SOR (Answer) on February 4, 2010.[2] He admitted all the SOR allegations, and requested a hearing to contest the adverse determination.

Over a year later, on May 12, 2011, the Government filed its ready-to-proceed. I was assigned the case on May 20, 2011 and, after coordinating with the parties, scheduled the hearing for July 26, 2011.[3] In order to promote the efficiency of the hearing, I issued a prehearing order requiring the parties to serve one another and me their expected exhibits and witness list prior to the hearing. The parties complied.

At hearing, the Government offered five exhibits, which were admitted as Government Exhibits (GE) 1 – 5. Applicant testified, called three witnesses, and submitted five groups of exhibits, which were admitted as Applicant's Exhibits (AE) A – E. The transcript was received on August 4, 2011.[4]

Findings of Fact

Applicant is 55 years old. He has been married since 1982 and has one child, who is now 25 years old. He attended the U.S. Air Force Academy (AFA) from 1973 to 1977, from which he graduated with a degree in engineering. He was then commissioned as an officer in the U.S. Air Force. Applicant spent the next 22 years in the Air Force, retiring in 1999, in the rank of lieutenant colonel (O-5).[5]

[1] This action was taken pursuant to Executive Order 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the Adjudicative Guidelines (AG) implemented by the Department of Defense on September 1, 2006. NATO employees and selectees, who are U.S. citizens and "who hold or require NATO certificates of security clearance or security assurances for access to U.S. or foreign classified information," have their cases adjudicated under DoD Directive 5220.6. Directive, ¶ 3.1.

[2] The file copy of the Answer has a date of February 4, 2009, but Applicant confirmed this was a typographical error and the actual date he filed his Answer was February 4, 2010. Tr. at 243.

[3] The short delay in scheduling the hearing was due to scheduling conflicts. Also, Applicant initially indicated his intent to request a hearing overseas.

[4] On August 23, 2011, Applicant's counsel sent an e-mail noting some minor typographical errors in the transcript. The Government did not file an objection or note any discrepancies. Applicant's e-mail is made part of the record and is Hearing Exhibit (HE) I. I have corrected the file copy of the transcript to reflect the discrepancies noted in HE I. In addition, I have made the following additional two minor pen-and-ink changes: page 10, line 14: Applicant's Counsel, not Department Counsel responds, and page 109, line 3, it was the witness who responded to the question.

[5] GE 1; AE C-12; Tr. at 129-139. *See also*, B-3 and B-6.

Applicant was first granted a security clearance in 1973 when he entered the AFA. His Air Force career was primarily in the field of command, control, communications, computers, intelligence, surveillance and reconnaissance or, as it is commonly referred to nowadays, C4ISR. He was involved with classified projects and was granted a Top Secret clearance with access to Sensitive Compartmented Information (TS/SCI).[6] While a member of the U.S. Air Force, Applicant never had a security violation, nor mishandled classified information.[7] Applicant's earliest performance reports to his last one in the Air Force speak to his professionalism, work ethic, and exceptional judgment.[8] During the Bosnian conflict and while assigned to NATO, Applicant developed and implemented security procedures that protected sensitive U.S. technology, while simultaneously ensuring that the C4ISR assets displayed and recorded critical mission data.[9]

After retiring from the Air Force in 1999, Applicant was hired by a NATO Agency (Agency). This Agency generally provides an initial three-year employment contract to individuals they hire and, if the Agency is happy with the individual's work performance, a three-year extension. Most employees do not have their employment contracts renewed at the end of the six-year period. However, a select few, 20 to 25 percent of those hired, whose performance is outstanding, are retained. In September 2010, Applicant was offered and accepted a permanent position with the Agency.[10] He currently serves as the Agency's head portfolio manager for a multi-million dollar a year contract, which provides NATO forces, including those deployed to Afghanistan, with much needed capabilities.[11]

From about 1999 to about April 2008, Applicant served as both a program manager and an executive officer for the Agency. These two responsibilities kept Applicant extremely busy. It involved a lot of paperwork, with other Agency employees coming in and out of Applicant's office, and leaving all sorts of papers on his desk. The Agency has since bifurcated these demanding positions and hired two different individuals to handle them. During this time, Applicant also shared an office with two other Agency employees. These two other employees reflected the Agency's culture at the time when it came to the handling and safeguarding of classified information. In short, employees at the Agency had become lax in their security responsibilities. The

[6] Tr. at 131-133, 165-166, 206-208. Applicant's officer performance reports note that he worked on and had access to highly classified U.S. technology. *See*, *e.g.*, C-23 – C-25 (managed Joint STARS program from 1983 to 1985); C-34 at 2 (provided briefings on technical aspects of F-22 Raptor in 1995). *See also*, AE C-2.

[7] Tr. at 165-166, 206-208. *See also*, GE 2, Response to Question 3.

[8] AE C-13 – C-39. See also, AE D-1 – D-5.

[9] AE C-37 at 1, *Impact on Mission Accomplishment*.

[10] Tr. at 35-37, 54-55, 135-142; AE C-1 – C-11.

[11] Tr. at 30-32.

security of classified information had taken a back seat to other priorities. Also, the fact that the Agency was physically located within a well-guarded restricted area where only authorized individuals were allowed to enter contributed to this lax attitude. It is during this period that the bulk of the security violations at issue occurred.[12]

The majority of Applicant's security violations took place between 1999 and 2005. (SOR, ¶ 1.a – 1.d). All were a result of negligence. Most were either actually committed by the two employees Applicant shared an office with or heavily contributed to by their actions or those of other Agency employees. Applicant, as the highest ranking individual in the shared office, always took responsibility for the violations. After one of the earlier incidents, Applicant spoke to the two employees about being more careful in securing classified material; however, he was not their supervisor. Following this conversation, one of the officemates improved her security awareness, while the other, who understood that Applicant would always be held responsible for the violations occurring in the shared workspace, did not change.[13] The new security manager for the Agency described this other employee as one of the worst offenders in handling and safeguarding classified information within the Agency.[14]

All the security violations that occurred between 1999 and 2005 involved NATO Restricted (NR) documents, except for a May 2004 incident involving NATO Confidential materials.[15] (SOR, ¶ 1.b). The Agency could not determine whether it was actually Applicant or one of the two officemates who committed the May 2004 violation.[16]

The last three security violations took place between 2006 and 2008. (SOR, ¶ 1.e – 1.g). The first of these in July 2006 occurred when Applicant returned from a trip and a secretary left a large number of documents on his desk for his review. One of these documents contained NR information, but did not have the required cover sheet alerting the reader that it was a NR document. Applicant quickly reviewed the documents, removed those classified documents that had the required coversheet, and threw out

[12] Tr. at 33-34, 47-50, 71-95, 105-106, 127-128, 150, 153-160, 174-176, 208-209. *See also*, AE A-3 – A-5 (physical security layout).

[13] Tr. at 34, 64-66, 97-100, 122-123, 174-194. *See also*, AE A-2 at 3 (Agency Report notes that "whenever a breach of security occurred in his multi-user office, (Applicant) admitted that he could not be sure that he alone was responsible but, as the senior person in the office, he accepted full responsibility for the breach under investigation."

[14] Tr. at 127-128.

[15] NATO has four levels of classification: Restricted, Confidential, Secret, and Top Secret. This generally causes problems for NATO employees with a U.S. background, because the U.S. does not have a true equivalent to NR. NATO employees with a U.S. background usually overlook that NR is a classification level requiring that the user handle and safeguard the information as they would other classified material. (Tr. at 88-90, 112-114).

[16] Tr. at 98-99 and 123-124. *See also*, AE A-2.

the rest, including the NR document, in his trash can. The Agency's security staff uncovered the violation and cited Applicant.[17] The last two security violations, in October 2006 and February 2008, involved NATO Secret (NS) material. In both instances Applicant was distracted by work, either a late business call or a meeting, and did not realize that the safe he shared with three other Agency employees had not been properly secured by one of the other employees. The other Agency employee had closed the safe, but forgotten to take the last step of spinning the dial. These violations were caught by the Agency's security staff and, as Applicant was the last to leave the office, he was held responsible for these violations.[18]

Shortly after the February 2008 incident, Applicant received a written warning from the Agency's Deputy General Manager. This served as a wakeup call to Applicant. Prior to this written warning, Applicant had only received, at most, a mild rebuke from a security officer or his supervisor regarding his past violations. Applicant was also placed on a one-year probationary period and the Security Manager told his staff to pay special attention to Applicant. The security staff did not detect any security violations by Applicant during the one-year probationary period, nor since the last incident in February 2008.[19]

Applicant has taken a number of steps to ensure that such violations do not occur again. He diligently follows a step-by-step checklist and then goes through the checklist a second time, to include checking his trash every night before he leaves to make sure that neither he, nor anyone else has mistakenly thrown away a classified document.[20] Since the last incident in February 2008, Applicant occupies his own office and the Agency hired an individual to take over his executive officer duties, which allows Applicant to concentrate on his program manager responsibilities.[21] The Security Manager, who has over two decades of experience in the security field, testified that he has no doubt as to Applicant's reliability and thinks "it highly unlikely that he (Applicant) would violate (security protocols) again."[22]

The Agency's Financial Controller and Director of Resources (Director), who has been delegated the security responsibility for the entire Agency, testified that all of Applicant's security violations were determined by the Agency to be minor. None were intentional and none resulted in the compromise of classified information. According to the Agency's own security rules, minor security violations, such as those at issue in this

[17] Tr. at 146-149, 194-195; GE 3 at 2.

[18] Tr. at 143-145, 195-206; GE 3 at 2-3.

[19] Tr. at 96-97, 110-111, 160-161, 188-191. *See also*, Tr. at 96-97 and 111-117.

[20] Tr. at 161-165. *See also*, Tr. at 115; AE B-5 (co-worker observes that Applicant complies with Agency's clean desk policy).

[21] Tr. at 97-100, 156-160.

[22] Tr. at 121. *See also*, Tr. at 70-71 (detailing Security Manager's extensive experience).

case, that are more than three years old are removed from an employee's file. All of Applicant's security violations have been removed from his record at the Agency.[23]

The Agency conducted its own investigation into Applicant's security violations. The subsequent report notes the lax security culture existing at the time of these security violations, and that a number of "Environmental Issues" contributed to the security violations at issue, to include Applicant being located in a "multi-user office." The report concludes that:

> Since the last incident . . . (Applicant) has occupied a single person office and has not been involved in any security violation. On the contrary, he has been fully cooperative, compliant and wholly conscious of the individual and collective part he plays in securing NATO's collective material and personnel. At no time was he ever considered a case that needed to be reported either to the National Security Authority or to the NATO Office of the Security, and this view was fully explained to the Federal Investigator during her visit to the Agency in June 2008. (Applicant) is currently seen as a well-respected and security conscious individual, who has learned from his previous mistakes.[24]

Applicant's immediate supervisor, a retired one-star flag officer, who has supervised Applicant over the last two years and gotten to know Applicant quite well, both on a professional and social level, testified on his behalf. He testified that Applicant has exceptional attention to detail and does not allow the fast pace of his work to undermine his security obligations. Based upon his observations, the supervisor opined that Applicant is totally reliable, has a strong character, and is a pivotal member of his team. As far as personnel security is concerned, the supervisor testified as to how Applicant serves as a role model to others[25] – testimony that was corroborated by both the Director and Security Manager.[26]

The General Manager of Applicant's Agency, a retired three-star general, writes: "I do not regard (Applicant) as a security risk in any way and would therefore urge that, in this case, his security clearance is left undisturbed and he be allowed to continued working within (the Agency)."[27] The Agency's former General Manager, who has known

[23] Tr. at 50-51, 63-66. *See also*, AE A-7 (Director's biography); Tr. at 115-121 (Security Manager testifies that the Agency's three-strike rule was never considered because none of Applicant's security violations were intentional and none involved the compromise of classified information. The security violations in this case did not rise to the level of damaging national security.).

[24] AE A-2.

[25] Tr. at 29-37, 39-41; AE A-8 (Supervisor's biography); AE B-2.

[26] Tr. at 53-54 and 66-67 (Director describes Applicant as being conscientious regarding his security responsibilities, having a great attitude towards his security obligations; and helps promulgate the new vigilant security culture at the Agency by mentoring others). *See also*, Tr. at 96-97.

[27] AE A-1.

Applicant since 1994, writes that "I have always found (Applicant) completely trustworthy and reliable. I have never had any occasion to question his dedication to his work, his loyalty or his integrity."[28]

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 to be used 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, administrative judges apply the guidelines 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 the applicant or proven by Department Counsel." The applicant has the ultimate burden of persuasion to obtain 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 safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation of potential, rather than actual, risk of compromise of classified information.

[28] AE B-4.

Section 7 of EO 10865 provides that adverse 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 Directive sets forth the security concern when an applicant fails to comply with rules and regulations regarding the handling of protected information at AG ¶ 33:

> 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 Appeal Board has held that "[o]nce it is established that an applicant has committed a security violation, he has a very heavy burden of demonstrating that he should be entrusted with classified information."[29] Accordingly, DOHA administrative judges must review any claims of reform and rehabilitation under a strict scrutiny standard.[30] Applicant's admissions in his affidavit (GE 3), interrogatory response (GE 2), and Answer, establish the 14 security violations alleged in the SOR. Thus, the "very heavy burden" standard enunciated by the Appeal Board applies.

After a review of the evidence, I concur with the position of the parties that the only two disqualifying conditions established by the evidence are AG ¶ 34(g)[31] and (h).[32] (Tr. at 224 and 232).

An applicant may mitigate the Guideline K concerns by establishing one or more of the mitigating conditions listed under AG ¶ 35. As noted above, Applicant in this case shoulders a "very heavy burden" in attempting to establish any of these mitigating conditions and his ultimate burden of persuasion under the Directive. I have considered all the mitigating conditions under AG ¶ 35, and find that the following warrant discussion:

---

[29] ISCR Case No. 07-08119 at 3-4 (App. Bd. July 8, 2010). *See also*, ISCR Case No. 04-12742 at 3 (App. Bd. February 25, 2011); ISCR Case No. 06-21537 at 4 (App. Bd. Feb. 21, 2008); ISCR Case No. 04-05802 at 5 (App. Bd. June 13, 2007) (Dissenting Opinion).

[30] *Id*. at 4.

[31] Any failure to comply with rules for the protection of classified or other sensitive information.

[32] Negligence or lax security habits that persist despite counseling by management.

> (a) so much time has elapsed since the behavior, or it happened so infrequently or under such unusual circumstances that it is unlikely to recur or does not cast doubt on the individual's current reliability, trustworthiness, or good judgment; and
>
> (b) the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities;

Applicant's last security violation occurred in February 2008, over three years ago. Since then, he has not committed any further violations. However, time alone, without the occurrence of any further violations, would not be sufficient to carry the day in light of the "very heavy burden" standard that is applicable in this case. Applicant met this burden. After his last security violation, Applicant was subjected to an intense one-year probationary period during which time he was singled out for special observation by the Agency's security staff. Even though the staff was tasked with looking for any violations committed by the Applicant, they did not find a single security violation during that probationary period or afterwards.

Further, and more importantly, Applicant has fundamentally changed the behavior and attitude that led to the security violations in the first place. Notably, he scrupulously follows a checklist and goes over it twice, including checking his trash to make sure that neither he, nor another employee has mistakenly thrown away classified material. He has become a role model for other employees and is helping change the Agency's previously lax security culture. Clearly, the formal warning Applicant received in 2008 served as a much needed wakeup call, and he has since responded positively in discharging his security responsibilities.

In addition, the circumstances under which the vast majority of these unintentional, minor violations took place have significantly changed since they occurred. Applicant is no longer tasked with two highly demanding jobs. The Agency hired two different individuals for the two time-consuming jobs Applicant held when these violations occurred. More importantly, Applicant no longer shares an office with the other employees who either committed the violations at issue or heavily contributed to their occurrence. The salutary result the Agency hoped would take effect when it instituted these changes has been realized, as evidenced by the lack of security violations over the past three plus years.

I had an opportunity to not only observe Applicant as he was questioned by counsel, but also questioned him myself. I found him credible and straightforward. He takes full responsibility for the violations at issue, is remorseful for his past conduct, and clearly now takes his security obligations seriously. I come to the same conclusion shared by all the witnesses in this case, including the Agency's General Manager, that Applicant's past history of security violations no longer casts doubt as to his current reliability, trustworthiness, and good judgment.

The above factors were favorably cited to by the Appeal Board in upholding a decision for an applicant in ISCR Case No. 04-05802. (*See* ISCR Case No. 04-05802 at 3). In that case, the applicant's last security violation occurred just a year before the favorable hearing decision. Moreover, unlike the cited Appeal Board case, Applicant's employer in this case did not wait until the eve of the hearing to make the necessary changes to the environmental factors that heavily contributed to the violations at issue. The salutary result the Agency expected from making these changes is clearly evident as there have been no further security violations since the changes took effect over three years ago.[33] Furthermore, this is not a case where Applicant failed to take responsibility for the security violations at issue,[34] the violations here did not result in the actual compromise of classified information,[35] and none of Applicant's violations were due to intentional or willful security breaches[36] – all factors that the Appeal Board has previously cited in reversing favorable hearing level decisions.

Accordingly, for all the reasons set forth above, I find that AG ¶ 35 (a) and (b) apply. Furthermore, I find that Applicant has met the very heavy burden standard and mitigated the Guideline K concern.

Whole-Person Concept

Under the whole-person concept, an administrative judge must evaluate an applicant's eligibility for a security clearance by considering the totality of an applicant's conduct and all the relevant circumstances. An administrative judge should consider the nine factors listed at AG ¶ 2(a).[37] I have considered and given due weight to all the favorable and extenuating factors in this case. Applicant served this nation in the Air Force for over 20 years. He was granted access to and worked on some of the Air Force's most sensitive C4ISR technology and cutting-edge weapon systems. He never

[33] *Compare with*, ISCR Case No. 04-05802 at 6 (one of the reasons cited by the Dissent in its separate opinion was the fact that the changes instituted by applicant's employer "occurred, at most, two or three weeks prior to the hearing . . . (and) the lack of ability to evaluate whether the change has had the salutary results applicant's superiors were hoping (to achieve)").

[34] ISCR Case No. 06-21537 at 4 ("While there is record evidence that Applicant is now more reliable, there is also evidence that Applicant has not demonstrated a positive attitude by downplaying her responsibility in the account's security errors.").

[35] *Id*. at 5 (agency determination that actual compromise occurred undermined Administrative Judge's favorable decision).

[36] ISCR Case No. 07-08119 at 5 (Appeal Board reverses due to evidence of an "ongoing pattern of knowing and willful security violations, in contradistinction to Applicant's contention of merely inadvertent breaches.").

[37] (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.

once violated security regulations during that time or compromised the security of these programs. The minor, inadvertent NATO security violations at issue here were a result of Applicant's prior workload, the lax security culture at the Agency, and sharing office space with others who, at times, willingly violated the security rules knowing Applicant would be held responsible. None of the violations resulted in the compromise of classified information, and the last security incident was over three years ago. Applicant's Agency is confident in his ability to continue to safeguard classified information and asks that he be granted a security clearance. Based upon all the evidence presented, as well as having the opportunity to observe and question Applicant, I am confident that he will continue to properly handle protected information. These whole-person factors, in conjunction with the favorable matters noted above, mitigate the Guideline K concern.

Overall, the record evidence leaves me with no questions or doubts about Applicant's eligibility and suitability for a security clearance.

Formal Findings

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

Paragraph 1, Guideline K (Handling Protected Information):	FOR APPLICANT
Subparagraphs 1.a – 1.h:	For Applicant

Conclusion

In light of all of the foregoing, it is clearly consistent with the national interest to grant Applicant continued access to classified information. Applicant's request for a security clearance is granted.

_____
Francisco Mendez
Administrative Judge