DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
[Redacted]	)	ISCR Case No. 10-00003
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Caroline Jeffreys, Esq., Department Counsel
For Applicant: Greg D. McCormack, Esq., and Jared McCormack, Esq.

December 15, 2011

Decision

FOREMAN, LeRoy F., Administrative Judge:

This case involves security concerns raised under Guidelines K (Handling Protected Information), E (Personal Conduct), and J (Criminal Conduct). Guideline K security concerns are mitigated, but security concerns under Guidelines E and J are not mitigated. Eligibility for access to classified information is denied.

Statement of the Case

Applicant submitted a security clearance application (SCA) on February 10, 2009. On May 25, 2011, the Defense Office of Hearings and Appeals (DOHA) sent him a Statement of Reasons (SOR) detailing the basis for its preliminary decision to deny his application, citing security concerns under Guidelines K, E, and J. DOHA acted under Executive Order 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the adjudicative guidelines (AG) implemented by the Department of Defense on September 1, 2006.

Applicant received the SOR on June 14, 2011; answered it on July 1, 2011; and requested a hearing before an administrative judge. DOHA received the request on July 5, 2011. Department Counsel was ready to proceed on August 31, 2011, and the case was assigned to an administrative judge on September 9, 2011. It was reassigned to me on September 19, 2011, to consolidate the docket. DOHA issued a notice of hearing on September 27, 2011, scheduling it for October 19, 2011. I convened the hearing as scheduled. Government Exhibits (GX) 1 through 5 were admitted in evidence without objection. Applicant testified and submitted Applicant's Exhibits (AX) A through C, which were admitted without objection. DOHA received the transcript (Tr.) on October 27, 2011.

Findings of Fact

In his answer to the SOR, Applicant admitted the allegations in SOR ¶¶ 1.a-1.h, and he denied the allegations in SOR ¶¶ 2.a-2.f and 3.a. His admissions in his answer and at the hearing are incorporated in my findings of fact.

Applicant is a 49-year-old employee of a defense contractor. He has worked for his current employer since 1984. (Tr. 13.) He was an engineering program manager from August 2006 to December 2010. In January 2011, he was promoted to director of power and control system engineering, manufacturing, and logistics. (AX A at 1-2.) He first received a security clearance in 1984, and he received eligibility for access to sensitive compartmented information (SCI) in 2006. His SCI eligibility was administratively terminated in 2008. (Tr. 34.)

Applicant graduated from college in May 1984, with a bachelor's degree in aerospace engineering. (AX A at 3.) He received a master's degree in engineering mechanics in May 1988. (AX A at 4; Tr. 31.)

Applicant married in August 1985. He and his wife have two children. His wife was diagnosed with breast cancer in the spring of 2004, underwent three surgeries and chemotherapy, and her cancer is in remission. (Tr. 28-29.)

Applicant's son, now 21 years old, was born 11 weeks premature, suffered brain trauma at birth, suffers from cerebral palsy, and is dependent on an electric scooter or wheelchair. He will graduate from college in the spring of 2012 and intends to begin working for Applicant's employer. (Tr. 29-30.)

Applicant's daughter, now 18 years old, is a college freshman. She suffers from scoliosis of the spine and underwent extensive corrective surgery in 2006. She has some decreased range of motion but no significant disability. (Tr. 30-31.)

Applicant's father worked for the Applicant's employer for 30 years, held a security clearance during his employment, and retired in 1992. In 2007, his father underwent surgery to remove a malignant tumor from his kidney. (Tr. 27, 36.)

In 1999 through 2001, Applicant was rated as "Excellent," the highest rating. In 2002, he received a 4.4 rating on a 5-point scale. In 2003, he received a 3.94 on a 4-point scale. The record does not contain his ratings for 2004-2006. His most recent ratings, on a 4-point scale, were 3.2 in 2007, 3.04 in 2008, 2.78 in 2009, and 2.76 in 2010. (AX A at 5-34.) Throughout his employment, he has received numerous cash awards and letters of appreciation. He most recently was selected to serve as an "ambassador" on the employees' political action committee. (AX A at 35-55.)

Around May 2003, shortly after being cleared for a special access program, Applicant exited a secure area with a single classified PowerPoint sheet that he had mingled with his unclassified papers. He discovered the classified sheet as he was walking back to his office. He immediately returned the classified sheet to the secure area, and he notified his security officer of his mistake. His security officer cautioned him to be more careful. No adverse action was taken against Applicant for this security violation. (GX 2 at 3; Tr. 37.)

A few days later, Applicant made the same mistake, mingling a single classified PowerPoint sheet with his unclassified materials. He discovered his mistake when he returned to his office, and he immediately returned the classified sheet to the secure area. He did not notify his security officer of this second incident (GX 2 at 3.) He testified that he did not report the second incident because he assumed the security officer would say the same thing as on the previous occasion. He now realizes that he should have reported it. (Tr. 39.) He admitted that he was embarrassed by the second violation, but testified that he did not believe he would have been punished or reprimanded for it. (Tr. 64-65.) He disclosed the second violation during a polygraph examination in January 2007. (Tr. 65.)

Between March 2003 and May 2004, Applicant used floppy discs and compact discs to transfer data from his employer's unclassified computer system to a classified system. The prescribed procedure was to have the computer administrator perform a virus scan on the discs before uploading the data onto the classified system. On two or three occasions, when the computer administrator was not available, Applicant performed the virus scan himself, uploaded the data onto the classified system, and then destroyed the disc in accordance with the prescribed procedures. He testified that he asked a coworker what he should do when the computer administrator was not available, and the coworker advised him to scan the disc himself. (Tr. 45, 70-71.) He did not report his actions when they occurred, but he later disclosed them during a polygraph examination in 2007.

Between September 2006 and October 2007, while working as an engineering program manager, Applicant entered a special access facility (SAF)[1] on six to eight occasions with his employer-issued Blackberry device on his person. On each occasion, he left the SAF as soon as he noticed that he had his Blackberry on his person and

[1] The DOHA interrogatories and Applicant's responses of April 26, 2010, refer to the facility as a sensitive compartmented information facility (SCIF). At the hearing, Applicant testified that the facility was not a SCIF, but rather was a special access facility (SAF). (Tr. 59-61.)

secured it outside the SAF. He never used the Blackberry while in the SAF. He did not report these security violations to his security officer, except for the last occasion. (GX 2 at 4.) He testified that he reported the last violation because he had seen "multiple people do that." (Tr. 42.)

On one occasion in February 2007, Applicant entered a SCIF with a flash drive in his pocket. A coworker had found the flash drive on the floor of Applicant's car, and Applicant put it in his pocket to avoid damaging it. He did not use the flash drive while in the SCIF. When he discovered it in his pocket, he immediately left the SCIF, reported the incident to his security officer, and surrendered the flash drive. (Tr. 43-44.)

Applicant underwent two polygraph examinations in January 2007, one in July 2007, and one in April 2008. (Tr. 89.) During those examinations, conducted by another U.S. Government agency, he disclosed all of the above security violations. (GX 2 at 3-5.) The context and purpose of these polygraph examinations is not reflected in the record. There is no evidence that any of the violations resulted in a compromise of classified or sensitive information.

When Applicant submitted his SCA in February 2009, he answered "No" to question 27b, asking, "In the last 7 years, have you illegally or without authorization modified, destroyed, manipulated, or denied others access to information residing on an information technology system?" On the same SCA, he answered "No" to question 27c, asking, "In the last 7 years, have you introduced, removed, or used hardware, software, or media in connection with any information technology system without authorization, when specifically prohibited by rules, procedures, guideline, or regulations?" He did not disclose that he uploaded information from an unclassified disc onto a classified system without having a virus scan performed by the computer administrator. At the hearing, he testified that he did not disclose this incident because at the time of the incident he thought he was authorized to perform the virus scan himself and he thought the question pertained only to intentional violations. (Tr. 47-50.)

In May 2009, Applicant was interviewed by a security investigator regarding his SCA. The investigator's summary of that interview includes the following:

> He states he has never deliberately falsified or concealed any relevant material on any form used to conduct investigations or to determine security clearance eligibility. He states he has never gave (sic) false or misleading information to anyone while being investigated for a security clearance. He states he has never removed any classified information from any approved facility, without proper authorization. He states he has never been cited for any security violation. He states he has never been denied a position of trust or removed from a position of truest.
>
> The subject states he has never illegally, without proper authorization, entered into, modified, destroyed, manipulated, or denied others access to any information technology. He states he has never introduced or

> removed any software, hardware or other media into any information technology system without authorization or in violation of any rule or other guideline.
>
> The subject did not have any questions of the investigator and advised he does not have anything relevant to add to this interview. The subject states he was not aware of any person or record that would contradict his statements. . . .

(GX 4 at 3-4.) Applicant did not disclose the two occasions in which he removed classified PowerPoint sheets from a secure area, the six or eight times he brought his Blackberry into a SAF, the one time he brought an unauthorized flash drive into a SCIF, or the occasions where he uploaded materials onto a classified system without having a virus scan performed by the computer administrator.

In response to DOHA interrogatories in May 2010, Applicant confirmed the accuracy and completeness of the investigator's summary but offered the following clarifications:

> In summary paragraph 5, to the question of "removing classified information from any approved facility, without proper authorization," my understanding of the question when I answered was that this question pertained to intentional removal. As I answered in my [response to previous DOHA interrogatories], the two incidents in question were unintentional and were reported previously to the Government. I am not claiming that this question as written in the investigator's report is inaccurate, but just my understanding of the question that led to my answer.
>
> In summary paragraph 6, pertaining to the question of ". . .has never introduced or removed any software, hardware or other media into any information technology system without authorization or in violation of any rule or other guideline." As I answered in my [response to previous DOHA interrogatories], my belief was that by performing the virus scan process myself, I was fulfilling the guideline for virus scanning.

(GX 3 at 6.)

Between October 2008 and October 2011, Applicant completed eight training sessions on information security awareness and special access programs requirements. (AX C.) He testified that he received additional training because of his previous security violations. (Tr. 53-54.)

A former supervisor, former subordinate, and four coworkers submitted written testimonials regarding Applicant's character. They uniformly described him as exceptionally talented, creative, conscientious, dedicated, and honest. They stated that

he has a reputation for attention to detail and security consciousness. They all were aware of the allegations in the SOR and uniformly supported continuation of Applicant's access to classified information. (AX C.)

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 have access to such information." *Id.* at 527. The President has authorized the Secretary of Defense or his designee to grant applicants eligibility for access to classified information "only upon a finding that it is clearly consistent with the national interest to do so." Exec. Or. 10865, *Safeguarding Classified Information within Industry* § 2 (Feb. 20, 1960), as amended.

Eligibility for a security clearance is predicated upon the applicant meeting the criteria contained in the AG. These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, an administrative judge applies these guidelines in conjunction with an evaluation of the whole person. An administrative judge's overarching adjudicative goal is a fair, impartial, and commonsense decision. An administrative judge must consider all available, reliable information about the person, past and present, favorable and unfavorable.

The Government reposes a high degree of trust and confidence in persons with access to classified information. This relationship transcends normal duty hours and endures throughout off-duty hours. 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 about potential, rather than actual, risk of compromise of classified information.

Clearance decisions must be made "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." *See* Exec. Or. 10865 § 7. Thus, a decision to deny a security clearance is merely an indication 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 may disqualify the applicant from being eligible for access to classified information. The Government has the burden of establishing controverted facts alleged in the SOR. *See Egan*, 484 U.S. at 531. "Substantial evidence" is "more than a scintilla but less than a preponderance." *See v. Washington Metro. Area Transit Auth.*, 36 F.3d 375, 380 (4th Cir. 1994). The guidelines presume a nexus or rational connection between proven conduct under any of the criteria listed therein and an applicant's security suitability. *See* ISCR Case No. 92-1106 at 3, 1993 WL 545051 at *3 (App. Bd. Oct. 7, 1993).

Once the Government establishes a disqualifying condition by substantial evidence, the burden shifts to the applicant to rebut, explain, extenuate, or mitigate the facts. Directive ¶ E3.1.15. An applicant has the burden of proving a mitigating condition, and the burden of disproving it never shifts to the Government. *See* ISCR Case No. 02-31154 at 5 (App. Bd. Sep. 22, 2005).

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 (App. Bd. Dec. 19, 2002). "[S]ecurity clearance determinations should err, if they must, on the side of denials." *Egan*, 484 U.S. at 531; *see* AG ¶ 2(b).

Analysis

Guideline K, Handling Protected Information

The SOR alleges Applicant exited a secured area with a classified document on two occasions in May 2003 (SOR ¶¶ 1.a and 1.b), and that he failed to report the second violation to his security officer (SOR ¶ 1.c). It further alleges that he entered a classified area with an unapproved Blackberry device approximately eight times from about September 2006 to October 2007 (SOR ¶ 1.d), and that he failed to report these violations to his security officer (SOR ¶ 1.e). It also alleges that he entered a classified area with an unapproved flash drive on about February 15, 2007 (SOR ¶ 1.f). Finally, it alleges that on two or three occasions between March 2003 and May 2004, he performed unauthorized virus scans on discs and uploaded the scanned data files onto the classified network (SOR ¶ 1.g), and that he failed to report these violations to his security officer (SOR ¶ 1.h).

The SOR alleges that Applicant's security violations and failures to report them violated the 1995 and 2006 versions of the Department of Defense Manual 5220.22-M, National Industrial Security Program Operating Manual (NISPOM). The relevant paragraphs of both versions of the NISPOM are virtually identical. Paragraph 5-100 of the NISPOM makes contractors and individual employees responsible for safeguarding classified information entrusted to them, in their custody, or under their control. Paragraphs 1-300, 1-302, and 1-303 require contractors to report events that affect proper safeguarding of classified information and any loss, compromise, or suspected compromise of classified information.

The security concern relating to Guideline K is set out in: 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." Applicant's admissions establish two disqualifying conditions under this guideline: AG ¶ 34(b) ("collecting or storing classified or other protected information at home or in any other unauthorized location") and AG 34(g) ("any failure to comply with rules for the protection of classified or other sensitive information"). AG 34(h) ("negligence or lax security habits that persist despite counseling by management") is

not established because there is no evidence that Applicant was counseled about his negligent security habits.

Security violations are one of the strongest reasons for denying or revoking access to classified information. Once a security violation is established, an applicant has a heavy burden of demonstrating that he or she should be entrusted with classified information. Because security violations strike at the very heart of the industrial security program, an administrative judge must give any claims of reform and rehabilitation strict scrutiny. ISCR Case No. 03-02688 (App. Bd. Oct. 5, 2006).

Security concerns under this guideline may be mitigated if "so much time has elapsed since the behavior, or it has happened so infrequently or under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or good judgment." AG ¶ 35(a). Applicant's violations were numerous and did not occur under unusual circumstances. However, the first prong of this mitigating condition ("so much time has elapsed") is a closer call. It focuses on whether the conduct was recent. There are no "bright line" rules for determining when conduct is "recent." The determination must be based on a careful evaluation of the evidence. *See* ISCR Case No. 02-24452 at 6 (App. Bd. Aug. 4, 2004). If the evidence shows "a significant period of time has passed without any evidence of misconduct," then an administrative judge must determine whether that period of time demonstrates "changed circumstances or conduct sufficient to warrant a finding of reform or rehabilitation." *Id*.

Applicant's last security violation was in February 2007, and he promptly reported it. With the exception of his unauthorized virus scans in 2003 and 2004, all his violations were the product of negligence rather than deliberate acts. His violations occurred while he was somewhat distracted by serious medical issues among his family members. Starting in October 2008, he completed eight courses of instruction related to protecting sensitive and classified information. Since his last violation, he has received excellent performance appraisals and awards, and in January 2011 he was promoted to a senior management position. At the hearing, he was candid and remorseful about his security violations. Based on all the evidence, I conclude that the mitigating condition in AG ¶ 35(a) is established.

Security concerns under this guideline also may be mitigated if "the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities." AG ¶ 35(b). There is no evidence that Applicant was counseled about his violations, but he has received remedial security training, and he demonstrated a positive attitude toward his security responsibilities during his testimony. I conclude that this mitigating condition is established.

Finally, security concerns under this guideline may be mitigated if "the security violations were due to improper or inadequate training." AG ¶ 35(c). I conclude that this mitigating condition is not fully established because the record reflects that Applicant

was aware of his security responsibilities. There is some indication in the record that Applicant's unauthorized virus scans before uploading data onto a classified computer were due to lack of training about that procedure. However, in all his other violations, he knew he had committed a violation, immediately corrected the situation, and on some cases reported it. I conclude that AG ¶ 35(c) is applicable to his unauthorized virus scans but not to his other violations.

Guideline E, Personal Conduct

Applicant's security violations are cross-alleged as personal conduct in SOR ¶ 2.a. His failure to disclose his unauthorized virus scans on his SCA is alleged in SOR ¶¶ 2.b and 2.c. His failure to disclose to a security investigator that he removed classified information from a secure area without authorization is alleged in SOR ¶ 2.d. His failures to disclose to a security investigator that he took an unapproved Blackberry device into a classified area, took an unapproved flash drive into a classified area, and performed unauthorized virus scans on discs before uploading data onto a classified network are alleged in SOR ¶ 2.e. His failure to disclose to a security investigator that he performed unauthorized virus scans is alleged again in SOR ¶ 2.f.

The concern under this guideline is set out in AG ¶ 15 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.

Applicant's security violations, cross-alleged as personal conduct, establish two disqualifying conditions under this guideline:

> AG ¶ 16(c): credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any other 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 properly safeguard protected information; and
>
> AG ¶ 16(e): personal conduct, or concealment of information about one's conduct, that creates a vulnerability to exploitation, manipulation, or duress, such as . . . engaging in activities which, if known, may affect the person's personal, professional, or community standing.

The mitigating conditions relevant to Applicant's security violations are: AG ¶ 17(c) ("the offense is so minor, or so much time has passed, or the behavior is so

infrequent, or it happened under such unique circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment"); and AG ¶ 17(d) ("the individual has acknowledged the behavior and obtained counseling to change the behavior or taken other positive steps to alleviate the stressors, circumstances, or factors that caused untrustworthy, unreliable, or other inappropriate behavior, and such behavior is unlikely to recur"). For the reasons set out in the above discussion of Guideline K, I conclude that both of these mitigating conditions are established for Applicant's security violations and his failures to report them as required.

The relevant disqualifying condition for Applicant's failure to disclose his security violations on his SCA is AG ¶ 16(a): "deliberate omission, concealment, or falsification of relevant facts from any personnel security questionnaire." The relevant disqualifying condition for his failure to disclose his security violations during his May 2009 interview with a security investigator is AG ¶ 16(b): "deliberately providing false or misleading information concerning relevant facts to an employer, investigator, security official, competent medical authority, or other official government representative."

An act of falsification has security significance independent of the underlying conduct. *See* ISCR Case No. 01-19278 at 7-8 (App. Bd. Apr. 22, 2003). The mitigation of the underlying conduct has little bearing on the security significance of the falsification, particularly where there are multiple falsifications. ISCR Case No. 08-11944 at 3 (App. Bd. Aug. 15, 2011).

With respect to Applicant's SCA, he testified that he did not disclose the unauthorized virus scan and uploading of data onto a classified system because he thought the questions pertained only to intentional violations. Although the unauthorized virus scan was an intentional act, he believed at the time of the act that he was authorized to do it.

With respect to the May 2009 interview with a security investigator, Applicant stated in his response to the May 2010 interrogatories and in his testimony at the hearing that he did not disclose the two occasions when he removed classified material from a security area without authority, because he believed the security investigator's questions pertained only to intentional violations. The security investigator apparently did not ask specifically about the incidents involving the unauthorized virus scans, the Blackberry device, or the flash drive, but his summary does reflect that he asked Applicant if he had anything relevant to add to the interview and received a negative response.

When a falsification allegation is controverted, as in this case, the Government has the burden of proving it. An omission, standing alone, does not prove falsification. An administrative judge must consider the record evidence as a whole to determine an applicant's state of mind at the time of the omission. *See* ISCR Case No. 03-09483 at 4 (App. Bd. Nov. 17, 2004).

Applicant was not required to disclose the incidents involving the Blackberry, and the flash drive, or the unauthorized virus scan in response to question 27b on his SCA, because none of those incidents involved modification, destruction, manipulation, or denial of access to information. He was not required to disclose the incidents involving the Blackberry and flash drive in response to question 27c, because he did not introduce, remove, or use hardware, software, or media without authorization during those incidents. However, he was required to disclose the unauthorized virus scan and subsequent uploading of data in response to question 27c.

I found Applicant's explanation for his negative answer to question 27c on his SCA implausible and unconvincing. Question 27c is a straightforward question asking about acts that were illegal or without authorization. It does not ask whether the acts were intentional or negligent. Furthermore, Applicant is well educated, intelligent, and not a neophyte in the security-clearance process. He was aware of the importance of full disclosure during the security-clearance process. *See* ISCR Case No. 08-05637 (App. Bd. Sep. 9, 2010) (level of education and business experience relevant to determining whether failure to disclose information was intentional). I conclude that Applicant's deliberately false answer to question 27c of his SCA establishes AG ¶ 16(a).

I also found Applicant's explanation for not disclosing his security violations during his May 2009 interview implausible and convincing. While he correctly told the investigator that he did not modify, destroy, manipulate, or deny others access to any information, he did not disclose his unauthorized virus scans and subsequently uploading of data when he was asked if he had ever entered into any information technology system without authority. He also did not disclose his unauthorized virus scans and uploading of data when he was asked if he introduced or removed any software, hardware, or other media into an information technology system without authorization. He was asked specifically about unauthorized removals of classified materials, but he did not disclose the two incidents in May 2003. He had been questioned about the incidents involving the Blackberry device, the flash drive, and the unauthorized virus scans during four polygraph examinations in 2007 and 2008, putting him on notice that they were matters of concern. Nevertheless, he answered in the negative when asked if he had anything relevant to add to the interview. I conclude that AG ¶ 16(b) is established.

Applicant's failure to disclose to the security investigator that he had uploaded data onto an information technology system without obtaining virus scans from the computer administrator is alleged twice, in both SOR ¶¶ 2.e and 2.f. When the same conduct is alleged twice in the SOR under the same guideline, one of the duplicative allegations should be resolved in Applicant's favor. *See* ISCR Case No. 03-04704 (App. Bd. Sep. 21, 2005) at 3 (same debt alleged twice). Thus, I have resolved SOR ¶ 2.e in Applicant's favor.

Security concerns raised by false or misleading answers on an SCA or during a security interview may be mitigated by showing that "the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being

confronted with the facts." AG ¶ 17(a). Applicant had an opportunity to correct his SCA during his May 2009 security interview, but he did not. He had an opportunity to correct his omissions during his May 2009 interview when he responded to DOHA interrogatories in May 2010, but he did not. I conclude that AG ¶ 17(a) is not established.

Security concerns raised by personal conduct may be mitigated if "the offense is so minor, or so much time has passed, or the behavior is so infrequent, or it happened under such unique circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment." AG ¶ 17(c). Applicant's intentional falsifications were not "minor." They were felonies, as discussed below under Guideline J, and they were intended to undermine the integrity of the security clearance process. They were recent, because they pertained to his current application to continue his clearance. They were not "infrequent" because he repeated them in his May 2009 interview, April 2010 responses to interrogatories, and at the hearing. They did not occur under unusual circumstances. I conclude that AG ¶ 17(c) is not established. No other enumerated mitigating conditions are established for Applicant's falsifications.

Guideline J, Criminal Conduct

Applicant's intentional failures to disclose his security violations on his SCA and during his May 2009 security interview are cross-alleged as criminal conduct under this guideline. The concern raised by criminal conduct is set out in AG ¶ 30: "Criminal activity creates doubt about a person's judgment, reliability, and trustworthiness. By its very nature, it calls into question a person's ability or willingness to comply with laws, rules and regulations." Disqualifying conditions under this guideline include "a single serious crime or multiple lesser offenses" and "allegation or admission of criminal conduct, regardless of whether the person was formally charged, formally prosecuted, or convicted." AG ¶¶ 31(a) and (c).

It is a felony, punishable by a fine or imprisonment for not more than five years, or both, to knowingly and willfully make any materially false, fictitious, or fraudulent statement or representation in any matter within the jurisdiction of the executive branch of the Government of the United States. 18 U.S.C. § 1001. Security clearances are matters within the jurisdiction of the executive branch of the Government of the United States. A deliberately false answer on an SCA or during a security interview is a serious crime within the meaning of Guideline J. I conclude that Applicant's false answers on his SCA and during his security interview in May 2009 raise the disqualifying condition in AG ¶ 31(a).

Security concerns under this guideline may be mitigated by evidence that "so much time has elapsed since the criminal behavior happened, or it happened under such unusual circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment." AG ¶ 32(a). For the reasons

set out in the above discussion of AG ¶ 17(c), I conclude that this mitigating condition is not established.

Security concerns raised by criminal conduct also may be mitigated if "there is evidence of successful rehabilitation; including but not limited to the passage of time without recurrence of criminal activity, remorse or restitution, job training or higher education, good employment record, or constructive community involvement." AG ¶ 32(d). Applicant expressed remorse for his security violations, but not for his falsifications. He persisted in his implausible explanation for his falsifications at the hearing. I conclude that this mitigating condition is not established. No other enumerated mitigating conditions under this guideline are established.

Whole-Person Concept

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. In applying the whole-person concept, an administrative judge must evaluate an applicant's eligibility for a security clearance by considering the totality of the applicant's conduct and all relevant circumstances. An administrative judge should consider the nine adjudicative process factors listed at AG ¶ 2(a):

> (1) the nature, extent, and seriousness of the conduct; (2) the circumstances surrounding the conduct, to include knowledgeable participation; (3) the frequency and recency of the conduct; (4) the individual's age and maturity at the time of the conduct; (5) the extent to which participation is voluntary; (6) the presence or absence of rehabilitation and other permanent behavioral changes; (7) the motivation for the conduct; (8) the potential for pressure, coercion, exploitation, or duress; and (9) the likelihood of continuation or recurrence.

I have incorporated my comments under Guidelines K, E, and J in my whole-person analysis. Some of the factors in AG ¶ 2(a) were addressed under those guidelines, but some warrant additional comment.

Applicant is well educated, intelligent, articulate, and talented. He has contributed to the national defense for many years. He is highly respected among his peers, supervisors, and subordinates. Nevertheless, his lack of candor during the security clearance process raises grave doubts about his trustworthiness, reliability, and good judgment. After weighing the disqualifying and mitigating conditions under Guidelines K, E, and J, and evaluating all the evidence in the context of the whole person, I conclude Applicant has mitigated the security concerns based on his handling of protected information, but he has not mitigated the security concerns raised by his lack of candor during the security clearance process. Accordingly, I conclude he has not carried his burden of showing that it is clearly consistent with the national interest to continue his eligibility for access to classified information.

Formal Findings

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

Paragraph 1, Guideline K:	FOR APPLICANT
Subparagraphs 1.a-1.h:	For Applicant
Paragraph 2, Guideline E:	AGAINST APPLICANT
Subparagraph 2.a-2.b:	For Applicant
Subparagraphs 2.c-2.d:	Against Applicant
Subparagraph 2.e:	For Applicant
Subparagraph 2.f:	Against Applicant
Paragraph 3, Guideline J:	AGAINST APPLICANT
Subparagraph 3.a:	Against Applicant

Conclusion

I conclude that it is not clearly consistent with the national interest to continue Applicant's security clearance. Eligibility for access to classified information is denied.

LeRoy F. Foreman
Administrative Judge