DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
[NAME REDACTED]	)	ISCR Case No. 10-05284
	)	
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Daniel F. Crowley, Esquire, Department Counsel
For Applicant: Greg D. McCormack, Esquire

04/12/2012

Decision

MALONE, Matthew E., Administrative Judge:

Applicant failed to mitigate the security concerns about his handling of protected information and about his personal conduct. His request for a security clearance is denied.

Statement of the Case

On December 2, 2008, Applicant submitted an Electronic Questionnaire for Investigations Processing (eQIP) to request a periodic review of his eligibility for a security clearance that is required as part of his employment. The results of the ensuing background investigation included information from an administrative inquiry (AI) into Applicant's conduct by the Defense Security Service (DSS). After reviewing the completed background investigation, adjudicators for the Defense Office of Hearings and Appeals (DOHA) sent interrogatories[1] to Applicant seeking to clarify or augment

[1] Authorized by DoD Directive 5220.6 (Directive), Section E3.1.2.2.

information contained therein. Based on his responses to the interrogatories and on the results of the background investigation, DOHA adjudicators were unable to find that it is clearly consistent with the national interest to continue Applicant's access to classified information.[2]

On September 20, 2011, DOHA issued to Applicant a Statement of Reasons (SOR), which contained a single allegation (SOR 1.a) of facts that raise security concerns addressed in the adjudicative guideline (AG)[3] for handling protected information (Guideline K). Applicant answered the SOR (Answer) on October 12, 2011, and requested a hearing. On November 3, 2011, Department Counsel sent to Applicant an *Amendment to the Statement of Reasons* (Amendment), which added a single allegation (SOR 2.a), citing as disqualifying personal conduct (Guideline E) the facts alleged at SOR 1.a. Applicant answered the Amendment on November 21, 2011.

The case was assigned to me on December 6, 2011, and I scheduled this matter to be heard on December 22, 2011. The parties appeared as scheduled. The Government presented seven exhibits (Gx.), which were admitted as Gx. 1 - 7. Applicant testified and proffered four exhibits (Ax.), which were admitted as Ax. A - D. DOHA received a transcript (Tr.) of the hearing on January 3, 2012.

Findings of Fact

The Government alleged under Guideline K (SOR 1.a) and Guideline E (SOR 2.a) that in November 2008, Applicant committed a security violation by failing to validate that an employee or subcontractor of his company had a security clearance required for access to a Navy facility, and that Applicant falsely represented to the Navy that the employee was cleared for access to that facility. Applicant denied the Government's allegations. Having reviewed the response to the SOR, the transcript, and exhibits, I make the following additional findings of fact.

Applicant is 40 years old and requires a security clearance for his position as a key management official of a small company doing business at several U.S. military facilities. Applicant and his wife were married in May 1994, and have two children, ages 17 and 9. Applicant served as an enlisted member of the U.S. Air Force from September 1995 until he was honorably discharged in September 1998. He was trained as a communications computer technician. After his discharge, he joined the U.S. Army Reserve, where he served in a similar capacity until his discharge in May 2006. Applicant has held a security clearance since about 1995. (Gx. 1; Ax. C; Tr. 21 - 26)

When Applicant was in the Air Force, he became friends with a civilian employed by a defense contractor doing information technology (IT) support work at the Air Force base where Applicant was assigned. After Applicant left active duty, he was hired by his friend's employer. They later decided to go into business together and, in April 2000,

[2] Required by Executive Order 10865, as amended, and by DoD Directive 5220.6 (Directive), as amended.

[3] The adjudicative guidelines were implemented by the Department of Defense on September 1, 2006. These guidelines were published in the Federal Register and codified through 32 C.F.R. § 154, Appendix H (2006).

incorporated as the company for which Applicant is now the chief financial officer (CFO). Until 2009, Applicant served as the company's primary facility security officer (FSO) and his friend was the CFO. The friend is now the company vice president and FSO. Applicant's wife also works for the company, and became company president in 2009. These are the only permanent, full-time employees of their company. (Gx. 7; Tr. 27 - 28)

Applicant's company provides IT support for military operating systems at military installations in the United States and abroad. The company's first contract was at a Navy shipyard, where Applicant started working as a company employee in 2000. Additionally, Applicant's company finds qualified IT personnel to work as independent civilian contractors at the shipyard, and at several military installations in the United States and abroad. The shipyard contracts for IT support and for staffing constitute his company's largest revenue source to date.

In a typical staffing transaction, Applicant's company identifies or is advised of a need for an IT specialist to work, for example, at the help desk for a base operating system. Applicant's company finds a suitable candidate and presents the person's qualifications to the military customer. If the candidate is appropriate, Applicant arranges an interview. Assuming the military approves the candidate to work at a site as an independent contractor, Applicant's company ensures that the person has or is processed for a security clearance. Applicant also handles all clearance-related paperwork, as well as payroll and other administrative matters related to the new hire. A person may sometimes work at the military site with an interim clearance based on a properly submitted eQIP. (Ax. A; Tr. 56 - 57)

Since 2000, Applicant's company has twice succeeded in renewing its contracts at the Navy shipyard where Applicant worked. In September and October 2008, Applicant's company was either preparing for or was in the process of bidding to renew the shipyard contract. Applicant was aware that he and his government counterpart did not work well together, and that his counterpart wanted to replace Applicant's company if possible. Applicant determined from speaking with government contract management officials that it would be easier to win the recompete bid if Applicant found an independent IT contractor as a replacement for his position, so Applicant could assume a less visible consulting role. (Tr. 28 - 32)

On October 17, 2008, Applicant identified and presented a suitable candidate to the shipyard. The candidate did not have a security clearance. This was the first such potential hire by Applicant's company that did not have a security clearance. The government customer liked the candidate and Applicant was directed to arrange for him to start work. That required submitting an eQIP and establishing an interim clearance for the candidate. On October 25, 2008, Applicant submitted a Visit Authorization Letter (VAL) required for the candidate to have access to the shipyard. The VAL, signed by the Applicant as the FSO, stated that the candidate had a secret level security clearance. (Gx. 3) The candidate was given a badge that allowed him access to the shipyard and he was given a workstation on site.

The candidate worked at the shipyard from October 28 until November 25, 2008. On November 4, the candidate requested an account for access to the shipyard's classified computer system. The shipyard security office accessed the Joint Personnel Adjudication System (JPAS) to verify the candidate's level of access. That inquiry showed that the candidate did not have a security clearance as stated on the VAL. On November 25, 2009, the candidate was interviewed, debriefed, and escorted from the shipyard.

On December 5, 2008, the shipyard security office reported Applicant's submission of the VAL to DSS as a security violation. A DSS Industrial Security Representative (ISR) subsequently conducted an AI into Applicant's actions, the shipyard's response, and the continued suitability of Applicant's company to conduct classified work through government contracts. (*Id.*) On December 9, 2008, the shipyard commander issued a Bar Order, whereby Applicant was ordered not to enter the shipyard. (Gx. 4)

The AI determined that Applicant deliberately submitted a VAL he knew to be invalid because Applicant did not submit the candidate's eQIP until November 10, about two weeks after he submitted the VAL. Applicant averred in his SOR response and in his testimony that he did not intentionally falsify the VAL. He claimed instead that he was not properly trained on the JPAS system, which he would have used to verify the candidate's clearance status. (Tr. 14 - 15, 35 - 36, 46 - 47, 60 - 61) The DSS AI determined that, at the time he submitted the VAL, Applicant had used JPAS for about three years. (Gx. 3)

In describing the search process that identified the candidate Applicant presented to the shipyard, Applicant testified that he was unable to find anyone meeting the job criteria who also held a security clearance. When the candidate went to the shipyard for an interview with Applicant's government counterparts, Applicant had to arrange for the candidate to have an escort because the latter did not have a clearance. (Tr. 33 - 34) However, on cross-examination, Applicant testified that he did not know the candidate did not have a security clearance when he submitted the VAL. (Tr. 49) I did not find Applicant's testimony on this point to be credible. I specifically find that Applicant knew his candidate did not have a security clearance when Applicant submitted the VAL.

After the AI was completed, DSS issued a report that found Applicant culpable in committing a security violation because he intentionally falsified the VAL needed for his candidate to work at the shipyard. However, the AI also concluded that there was no compromise of any classified or other sensitive information, and it listed several mistakes by the shipyard security office, including a lack of immediate response to the presence of a contractor on site who was not cleared to be there. (Gx. 3)

Follow-up actions included extensive remedial training for Applicant, which he completed in March 2009. (Ax. C) Additionally, DSS inspected Applicant's company in April 2009 and found several discrepancies, which Applicant's company promptly resolved. DSS recently rated as "satisfactory" the company's overall "effectiveness of the facility security posture" based on June 2010 and August 2010 inspections. (Gx. 2;

Ax. C) Few discrepancies were noted during those inspections. (Ax. C) All available information bearing on his current relationship with the shipyard, including an unsolicited letter from Applicant to the deputy commander (*Id.*), indicates the Bar Order against Applicant has not been lifted.

Applicant's business partner, as well as several current and former associates in the IT industry, support Applicant's continued access to classified information. They note his reliability, professional and personal integrity, and the value of his expertise to the military. (Ax. D)

Policies

A security clearance decision is intended to resolve whether it is clearly consistent[4] with the national interest for an applicant to either receive or continue to have access to classified information. Each decision must be a fair, impartial, and commonsense determination based on examination of all available relevant and material information,[5] and consideration of the pertinent criteria and adjudication policies in the adjudicative guidelines. Decisions must also reflect consideration of the factors listed in ¶ 2(a) of the new guidelines. Commonly referred to as the "whole-person" concept, those factors are:

> (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.

The presence or absence of a disqualifying or mitigating condition is not, by itself, conclusive. However, specific applicable guidelines should be followed whenever a case can be measured against them as they represent policy guidance governing the grant or denial of access to classified information. The Government bears the initial burden of producing admissible information on which it based the preliminary decision to deny or revoke a security clearance for an applicant. Additionally, the Government must be able to prove controverted facts alleged in the SOR. If the Government meets its burden, it then falls to the applicant to refute, extenuate or mitigate the Government's case. Because no one has a "right" to a security clearance, an applicant bears a heavy burden of persuasion.[6] A person who has access to classified information enters into a fiduciary relationship with the government based on trust and confidence. Thus, the government has a compelling interest in ensuring each applicant possesses the

---

[4] *See Department of the Navy v. Egan*, 484 U.S. 518 (1988).

[5] Directive. 6.3.

[6] *See Egan,* 484 U.S. at 528, 531.

requisite judgment, reliability, and trustworthiness of one who will protect the national interests as his or her own. The "clearly consistent with the national interest" standard compels resolution of any reasonable doubt about an applicant's suitability for access in favor of the government.[7]

Analysis

Handling Protected Information

By denying the allegation at SOR 1.a, the burden remained on the Government to support that allegation through sufficient reliable evidence. The Government carried its burden by establishing that Applicant committed a security violation in October 2008, when he submitted a VAL to a Navy shipyard that he knew to be false. When he presented the candidate for an interview at the shipyard, Applicant had to arrange for an escort because the candidate did not have a clearance. When Applicant submitted the VAL 10 days later, an eQIP had not yet been submitted that may have provided the candidate with an interim clearance to work at the shipyard. Applicant's conduct was deliberate and he knew or should have known, it was a breach of well-established security procedures.

The security concern raised by Applicant's conduct is expressed at AG ¶ 33, as follows:

> Deliberate or negligent failure to comply with rules and regulations for protecting classified or other sensitive information raises doubt about an individual's trustworthiness, judgment, reliability, or willingness and ability to safeguard such information, and is a serious security concern.

More specifically, available information requires application of the disqualifying condition at AG ¶ 34(g) (*any failure to comply with rules for the protection of classified or other sensitive information*). By contrast, the record also requires consideration of all of the AG ¶ 35 mitigating conditions, listed as follows:

> (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;
>
> (b) the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities; and
>
> (c) the security violations were due to improper or inadequate training.

[7] *See Egan;* AG ¶ 2(b).

The mitigating condition at AG ¶ 35(a) is only partially applicable, in that the events at issue occurred over three years ago. However, the circumstances surrounding Applicant's conduct were not unusual or unpredictable. To the contrary, they arose in the context of a key part of his business. Further, Applicant's continued insistence on his lack of JPAS training, and his conflicting testimony about his knowledge of the candidate's clearance status, undermine a conclusion that his past behavior does not cast doubt on his current good judgment.

AG ¶ 35(b) also is only partially applicable. Applicant successfully completed a remedial industrial security class in March 2009. Because his company has only two other employees, he also benefits from the fact his company corrected deficiencies found in a post-AI inspection and was recently found to be discrepancy-free in two 2010 inspections. However, Applicant's continued insistence that he did not deliberately submit a false VAL and that he did not have enough JPAS training precludes a conclusion that he now has a positive attitude toward security.

Finally, AG ¶ 35(c) does not apply. Applicant used JPAS for three years as part of a key facet of his business. He is an experienced IT professional and knew, or should have known, how to verify the candidate's security clearance status. Of course, his claim that he was not properly trained is wholly undermined by the fact that he knew at the outset the candidate had no clearance.

Applicant correctly argued that part of the reason the candidate had access to the shipyard when it first became known he did not have a clearance was that the shipyard security office did not conduct its own JPAS verification. He also averred that the severity of his violation is lessened by the fact that there was no compromise of protected information. Indeed, it is not clear why the shipyard security office did not act to remove the candidate sooner. But the Applicant's actions, not those of the shipyard security office, are at issue here. Further, the government need not wait until its information is lost or compromised before taking action. Adherence to proper procedures intended to safeguard classified information is paramount. A demonstrated willingness to disregard those procedures is sufficient for disqualification. On balance, Applicant has not mitigated the security concerns about his 2008 security violation.

Personal Conduct

The Government also established, despite Applicant's denial of SOR 2.a, that his actions raised a security concern about his personal conduct. That security concern is expressed at 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.

More specifically, the Government's information is sufficient to support application of the following disqualifying condition at 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.

Applicant knowingly provided false information to shipyard security officials about the candidate's security clearance status when he submitted the VAL. That information was provided to further Applicant's interest in resolving a personality conflict that could potentially hinder his company's efforts to keep the shipyard contract.

Of the mitigating conditions listed at AG ¶ 17, I considered the following as pertinent to these facts:

> (a) the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts;
>
> (b) the refusal or failure to cooperate, omission, or concealment was caused or significantly contributed to by improper or inadequate advice of authorized personnel or legal counsel advising or instructing the individual specifically concerning the security clearance process. Upon being made aware of the requirement to cooperate or provide the information, the individual cooperated fully and truthfully;
>
> (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
>
> (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.

AG ¶ 17(a) does not apply. Applicant submitted the VAL on October 27. Based on the VAL, the candidate was allowed to work at the shipyard from October 28 until November 25. The eQIP for the candidate was not submitted until November 10, something Applicant has yet to adequately explain. He has never admitted that he falsified the VAL by representing that the candidate had a secret clearance.

Also, for the same reasons the mitigating condition at AG ¶ 35(c) does not apply, AG ¶ 17(b) does not apply. Applicant's claim of inadequate training on a JPAS system he used for three years is not supported by the record as a whole.

Available information supports partial application of AG ¶¶ 17(c) and 17(d). Applicant's November 2008 security violation is the only known instance of misconduct, and it occurred more than three years ago. After the AI, Applicant completed remedial

industrial security training, and his company has been in compliance with DoD industrial security requirements since April 2009. However, for the same reasons I have doubts about Applicant's attitude regarding his security responsibilities, I am concerned that his failure to accept that his actions were deliberate and not due to faulty training, or other factors not of his making, will lead to similar decisions in the future. Applicant did not mitigate the security concerns about his personal conduct.

Whole-Person Concept

I have assessed the facts presented in this record and have applied the appropriate adjudicative factors under Guidelines E and K. I have also reviewed the record before me in the context of the whole-person factors listed in AG ¶ 2(a). Applicant is a veteran of the Air Force and Army, who has established a successful defense contracting business. He has a reputation for integrity and hard work, which, when coupled with his IT expertise and commitment to supporting various military missions, makes him a valuable asset to the defense industry.

Nonetheless, Applicant deliberately violated the government's trust when he submitted a false statement to gain access to a military facility for a new hire. His willingness to cut corners in furtherance of his business interests is fundamentally at odds with the government's personnel industrial security program. The rehabilitative value of his remedial training and his company's compliance efforts is negated by Applicant's unfounded denials. Doubts remain about Applicant's commitment to following basic procedures for safeguarding classified and other sensitive information. Because protection of the national interest is the overriding concern in these adjudications, those doubts must be resolved against the Applicant.

Formal Findings

Formal findings on the allegations set forth in the SOR, as required by section E3.1.25 of Enclosure 3 of the Directive, are:

Paragraph 1, Guideline K:	AGAINST APPLICANT
Subparagraph 1.a:	Against Applicant
Paragraph 2, Guideline E:	AGAINST APPLICANT
Subparagraph 2.a:	Against Applicant

Conclusion

In light of all of the foregoing, it is not clearly consistent with the national interest to continue Applicant's access to classified information. Request for security clearance is denied.

MATTHEW E. MALONE
Administrative Judge