



**DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS**



In the matter of:)
)
) ISCR Case No. 09-02821
)
)
Applicant for Security Clearance)

Appearances

For Government: Ray Blank, Esquire, Department Counsel

For Applicant: *Pro se*

January 13, 2011

Decision

O'BRIEN, Rita C., Administrative Judge:

Based on a review of the hearing transcript, pleadings, and exhibits, I conclude that Applicant has not mitigated the security concerns raised under the guidelines for use of information technology systems and personal conduct. Accordingly, his request to continue his security clearance is denied.

Statement of the Case

Applicant submitted an Electronic Questionnaire for Investigations Processing, which he signed on May 18, 2007. After reviewing the results of the ensuing background investigation, adjudicators for the Defense Office of Hearings and Appeals (DOHA) were unable to make a preliminary affirmative finding¹ that it is clearly consistent with the national interest to grant Applicant's request for a security clearance.

¹ Required by Executive Order 10865, as amended, and by DoD Directive 5220.6 (Directive), as amended.

On February 4, 2010, DOHA issued to Applicant a Statement of Reasons (SOR) that specified the basis for its decision: security concerns addressed in the Directive under Guideline M (Use of Information Technology Systems) and Guideline E (Personal Conduct) of the Adjudicative Guidelines (AG).² Applicant signed his notarized Answer to the SOR on March 6, 2010. Applicant requested a decision before an administrative judge. Department Counsel was prepared to proceed on August 10, 2010, and the case was assigned to me on August 23, 2010. DOHA issued a Notice of Hearing on September 1, 2010, and I convened the hearing as scheduled on September 15, 2010.

Department Counsel offered four exhibits, marked as Government Exhibits (GE) 1 through 4, which were admitted without objection. Applicant testified and offered 15 exhibits, marked as Applicant Exhibits (AE) A through O. Department Counsel objected to exhibits A through H and K as irrelevant. His objections go to weight rather than admissibility of the documents. I admitted Applicant's exhibits A through O. DOHA received the transcript (Tr.) on September 22, 2010.

Procedural Ruling

I take administrative notice of a federal statute, Title 18 U.S.C. § 704. I marked Department Counsel's brief related to the statute as Hearing Exhibit (HE) I, and Applicant's reply brief as HE II.³

Findings of Fact

In his Answer, Applicant admitted all of the SOR allegations, except 2.b. and 2.d., which he did not clearly admit or deny. At the hearing, he admitted both allegations. Applicant's admissions to the SOR allegations are incorporated herein as findings of fact. After a thorough review of the pleadings and the evidence, I make the following additional findings of fact. (Tr. 17-18)

Applicant is 65 years old. He divorced from his first wife in 1993. His three sons and one daughter from his first marriage are now adults, living independently. He remarried in 1995. He holds two masters degrees and a doctorate degree. His law degree was awarded in 2010. Applicant served as an Army officer in the National Guard from 1967 – 1978, after which he served in the reserves until 1994. His status changed to medically unqualified reservist from 1994 until his retirement in 2005, because of

² Adjudication of this case is controlled by the Adjudicative Guidelines that were implemented by the Department of Defense on September 1, 2006. The Adjudicative Guidelines supersede the guidelines listed in Enclosure 2 to the Directive, and they apply to all adjudications or trustworthiness determinations in which an SOR was issued on or after September 1, 2006.

³ In response to my order, Department Counsel submitted a post-hearing brief regarding 18 U.S.C. § 704. Subsequently, Applicant submitted a reply brief. (HE I, II)

orthopedic problems. He retired as a lieutenant colonel. During his military career, he did not serve overseas or in combat. He has held a security clearance continuously since at least 1970, including a top secret clearance since 1989. He has worked for his current employer since February 2007. (GE 1, 2; AE A, C, D; Tr. 46, 55, 77-78, 83-84)

In 1999, federal government agency A considered Applicant for the position of scientist in the computer-vulnerabilities section. Subsequently, an agent conducting Applicant's investigation spoke with Applicant's ex-wife and friends. In December 1999, the job offer was withdrawn. Wishing to learn the reason why the offer was withdrawn, Applicant submitted a Freedom of Information Act (FOIA) request in January 2000, and received a redacted copy of his investigative file. The file stated that he was being discontinued "based on his financial irresponsibility (reasons for filing bankruptcy, DFAS outstanding debt)." It also noted that "Applicant appears to pay child support only when taken to court and forced to do so. Also, he misrepresents his actual military accomplishments." (AE A; Tr. 42-43, 82)

In 2005, Applicant was assigned by his contractor-employer to work at federal agency A, the same agency that had previously rescinded its job offer. His job as a database designer and researcher at agency A involved reviewing cases and developing searches for information contained in computer files. For this position, Applicant was submitted for an upgrade to his clearance to permit access to sensitive compartmented information (SCI). His position gave him access to the automated files of members of the general public. Applicant used his position to search files, without authorization, to learn who had told agency A in 1999 that he failed to pay child support. Applicant gathered personal data "...by searching for himself; family members, prior employers, ex-wife and prior references" and also "misused [agency] systems on a regular basis..." He testified that he accessed the personal files of approximately 18 individuals. By searching these files, he learned that it was his ex-wife who had stated that he did not pay child support unless he was forced to do so through court action. At the hearing, he denied this accusation and submitted a 2010 letter from the attorney who handled his custody and child support case during the period 1996 to 1997. The attorney stated that Applicant met his child support obligations. Applicant submitted several documents related to his divorce proceedings. (GE 3; AE D-H; Tr. 41-46, 74-76, 80)

During the background investigation for this SCI upgrade, Applicant had a polygraph interview and examination in June 2006. The following month, Applicant was again interviewed, specifically in regard to the polygraph results. During this interview, Applicant denied that he searched his own or others' private computer files. The agency reported that Applicant "...failed to disclose his actions even when directly questioned." Later in the interview, Applicant admitted his unauthorized use of agency A's files. In September 2006, agency A's security program manager denied Applicant "further access to [agency A] facilities/information and projects/contracts." He cited Applicant's misuse of agency A's computer systems for personal data gathering, and referred the case to the DOD security clearance office. In the fall of 2006, his SCI access was

denied and he was released from his employment by the defense contractor. (GE 2, 3, 4; Tr. 44, 76)

Applicant testified that in the 1980s and 1990s, he told friends, family, and his children that he was a veteran of combat action in Vietnam, although he had never served there. The agency A interviewers in July 2006 said that Applicant

...would retell stories that he heard from fellow Guard and Reserve members who had served in Vietnam and would replace his name in the story as if he had experienced the events. He stated that he told stories about being ambushed and how he “got out” when in reality it was a story that had been told by a Sergeant in his Guard unit. (GE 4)

Applicant also admits that, during the 1980s and 1990s, he bought military medals and ribbons at flea markets and pawn shops, and wore them as if they had been awarded to him. He embellished his military background because he had volunteered for duty in Vietnam, but he had not been selected. He also noted that telling these stories “fed his ego.” At the hearing, he admitted that, as a military officer, he knew he was not allowed to purchase or wear military medals he had not earned. However, he also testified that he was not aware his actions violated the Uniform Code of Military Justice (UCMJ)⁴ or federal law.⁵ (GE 2, 4; Tr. 68-69, 76-77, 79)

Applicant testified that immediately after his July 2006 polygraph interview, he prepared a list of the issues raised during the interview and provided it to his supervisors and security manager. The list includes two statements about the conduct alleged in the SOR:

⁴ Under Article 134 of the UCMJ, it is a criminal offense for those subject to the UCMJ to wear unauthorized decorations on a uniform or civilian clothing. Applicant contends in his brief that he was not subject to the UCMJ during most of his life. Violation of Article 134 is not alleged in the SOR, and therefore, will only be considered as part of the whole-person analysis. (See ISCR Case No. 03-20327 at 4 (App. Bd. Oct. 26, 2006); HE I, II)

⁵ In 2006, Congress passed 18 USCS § 704, commonly called the Stolen Valor Act. It expanded a 1948 law that prohibited wearing unearned military medals and decorations. It added a prohibition against making false verbal or written claims about such awards (subsection [b]). In 2010, the 9th Circuit Court of Appeals found subsection (b) unconstitutional on free speech grounds. (See *U.S. v. Alvarez*, 2010 U.S. App., LEXIS 17135, Aug 17, 2010) Also in 2010, a federal district court in Colorado dismissed charges against a man who claimed to have been awarded the Purple Heart and Silver Star. The court found subsection (b) unconstitutional on the same grounds as the *Alvarez* court. (See *U.S. v. Strandlof*, 2009 WL 5126540 (D.Colo. Dec. 18, 2009). Neither of these decisions discussed subsection (a), which concerns the wearing of military decorations. Subsection (a) was challenged in *U.S. v. McGuinn*, 2007 U.S. App., LEXIS 77059 (SDNY). The court held that § 704(a) is not unconstitutionally vague or overbroad. Applicant states in his brief that the statute was not in effect in the 1980s and 1990s when he engaged in the subject activity. Although subsection (b) was not enacted until 2006, the earlier version of 18 USC § 704, which prohibits wearing unearned military decorations (and corresponds to the current subsection [a]), has been in effect since at least 1948. Violation of 18 USC § 704 is not alleged in the SOR, and therefore, will only be considered under the whole-person analysis. (See ISCR Case No. 03-20327 at 4 (App. Bd. Oct. 26, 2006); HE I, II)

Researched my [agency] file in ACS [computer system] and tried to see if it was being updated. Viewed file and associated files, thought I covered issue but not to [agency] satisfaction.

Did embellish military history in unofficial settings. (GE 2)

He met with his supervisor and security manager for about one hour to discuss the polygraph interview. He thinks he told some friends about his military fabrications, but could not provide names or dates. At his current company, he also provided the same one-page list to his supervisor and security officer, but has not discussed the allegations in the current adjudication. (GE 2; AE M; Tr. 39-41, 63-68)

Applicant has not received counseling. He has engaged in “a lot of reflection” and realizes his behavior was “stupid,” “idiotic,” and “problematic,” and stated that it will not occur again. During the course of his investigation, he did not provide the underlying reasons why he lied about his service or wore unearned decorations because, “I felt that the act had happened and the reasons that it happened at the time and under those circumstances of questioning were largely irrelevant.” At the hearing, he explained that the underlying cause was his feeling of inadequacy growing up, which led him to join the National Guard and volunteer for active duty. He did not serve on active duty because “I would have had to resign my commission and go through OCS again, which I chose not to do.” (GE 2; AE M; Tr. 39-41, 65-72)

Applicant provided a character reference from his supervisor at the company where his SCI was revoked. He has known Applicant for six years. Applicant is his friend and his landlord. When Applicant’s SCI access was suspended, the writer did not observe any adverse or security-significant behavior. He does not know why Applicant’s access was suspended. He finds Applicant to be a tireless worker and notes Applicant’s work with volunteer organizations. He believes Applicant has a zeal to achieve and a sense of dedication. Applicant’s performance reports from 1980 to 1996 describe him as a top performer, leader and manager, and a loyal and dedicated officer, with ethics beyond reproach. (AE I, L; Tr. 51)

Policies

Each security clearance decision must be a fair, impartial, and commonsense determination based on examination of all available relevant and material information, and consideration of the pertinent criteria and adjudication policy in the revised AG.⁶ Decisions must reflect consideration of the “whole-person” factors listed in ¶ 2(a) of the Guidelines.

⁵ Directive. 6.3.

The presence or absence of disqualifying or mitigating conditions does not determine a conclusion for or against an applicant. However, specific applicable guidelines should be followed when a case can be so measured, as they represent policy guidance governing the grant or denial of access to classified information.

A security clearance decision is intended only to resolve the question of whether it is clearly consistent with the national interest⁷ for an applicant to receive or continue to have 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. Additionally, the Government must be able to prove controverted facts alleged in the SOR. If the Government meets its burden, it falls to applicants to refute, extenuate or mitigate the Government's case. Because no one has a "right" to a security clearance, applicants bear a heavy burden of persuasion.⁸ A person who has access to classified information enters a fiduciary relationship based on trust and confidence. The Government has a compelling interest in ensuring that applicants possess the requisite judgment, reliability, and trustworthiness to protect the national interest 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 to classified information in favor of the Government.⁹

Analysis

Guideline M, Use of Information Technology Systems

AG ¶ 39 expresses the security concern about use of information technology systems:

Noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual's reliability and trustworthiness, calling into question the willingness or ability to properly protect sensitive systems, networks, and information. Information Technology Systems include all related computer hardware, software, firmware, and data used for the communication, transmission, processing, manipulation, storage, or protection of information.

AG ¶ 40 describes disqualifying conditions that could raise a security concern, including the following relevant condition:

⁶ See *Department of the Navy v. Egan*, 484 U.S. 518 (1988).

⁷ See *Egan*, 484 U.S. at 528, 531.

⁸ See *Egan*; Revised Adjudicative Guidelines, ¶ 2(b).

(e) unauthorized use of a government or other information technology system.

While assigned to work at a federal agency, Applicant had access to the personal files of the general public. Although he was not authorized, Applicant accessed his own file, and the personal files of prior employers, prior references, family members, and his ex-wife. Disqualifying condition AG ¶ 40(e) applies.

AG ¶ 41 provides the following relevant mitigating conditions:

(a) so much time has elapsed since the 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;

(b) the misuse was minor and done only in the interest of organizational efficiency and effectiveness, such as letting another person use one's password or computer when no other timely alternative was readily available; and

(c) the conduct was unintentional or inadvertent and was followed by a prompt, good-faith effort to correct the situation and by notification of a supervisor.

Applicant used a government agency computer to view other people's personal files in 2005, which is not recent. Given the repercussions of his actions, he is unlikely to engage in such actions again. However, Applicant use of his position to satisfy his personal desire to see information about his former wife, family, and friends, indicates a lack of trustworthiness. His actions occurred during the course of his routine duties, not in unusual circumstances. Only partial mitigation is available under AG ¶ 41(a). Moreover, Applicant's conduct was neither minor nor inadvertent: he violated the privacy of approximately 18 individuals to satisfy his own desires to determine the source of certain information. He committed serious and intentional breaches of the trust placed in those with access to private information. Applicant made no effort to inform authorities at the time he accessed these files. Only as a result of his polygraph interview in 2006 did he inform his supervisor and security officials. Although this conduct occurred several years ago, the deliberate nature of Applicant's actions and the gravity of his breach of trust outweigh their distance in time. Partial mitigation under AG ¶ 41(a) is insufficient to find for Applicant under Guideline M.

Guideline E, Personal Conduct

AG ¶ 15 expresses the security concern about personal conduct:

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.

AG ¶ 16 describes conditions that could raise a security concern and may be disqualifying. The following conditions are relevant:

(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

(e) personal conduct, or concealment of information about one's conduct, that creates a vulnerability to exploitation, manipulation, or duress, such as (1) engaging in activities which, if known, may affect the person's personal, professional, or community standing...;

In 2005, Applicant deliberately searched computer files containing private information which he was not authorized to access. He did not inform his employer, or federal agency A, of his unauthorized actions. During his 2006 agency A interview, he initially did not disclose his actions to the investigators, even when directly asked. He only disclosed it subsequently, when asked again during the interview. He did not disclose his actions to his employer until after that same interview. Applicant's conduct, both in searching private files, and in hiding his behavior, demonstrate untrustworthiness, lack of candor, and unwillingness to follow rules. His false tales of his combat experience, and wearing medals he had not earned, underscores his poor judgment and willingness not only to engage in falsehoods, but to continue the fabrications over many years. AG 16(c) applies.

During the time between 2005 and 2006, before his disclosures, Applicant was vulnerable to exploitation or coercion, because disclosure of this information would have had a significant negative effect on his reputation and career. Moreover, over the course of two decades, he was vulnerable to coercion because any revelation that he embellished his military accomplishments, related false tales of his combat service in Vietnam, and wore military medals and decorations that he did not earn, would have tarnished his community standing and reputation. AG ¶ 16(e) applies.

AG ¶ 17 provides conditions that could mitigate security concerns under the Personal Conduct guideline. The following conditions are relevant:

(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

(e) the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress.

AG ¶ 17(c) does not apply, for the reasons discussed under Guideline M. Regarding mitigating condition AG ¶ 17(e), Applicant testified that he revealed his conduct to his employer in 2006, and to his current employer as well. It appears he is no longer vulnerable to exploitation. However, his disclosure must be viewed in light of its timing. He disclosed the behaviors listed in the SOR to his supervisor and security officer only after he was questioned about them at his interview in 2006. His lack of disclosure until that point indicates that he was acting in response to the security clearance process rather than as a good-faith effort to be forthright about his behavior.

Whole-Person Analysis

Under the whole-person concept, an administrative judge must evaluate the Applicant's security eligibility by considering the totality of the Applicant's conduct and all the 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.

AG ¶ 2(c) requires that the ultimate determination of whether to grant a security clearance be an overall commonsense judgment based upon careful consideration of the guidelines and the whole-person concept. Under the cited guidelines, I considered the potentially disqualifying and mitigating conditions in light of all the facts and circumstances surrounding this case.

Applicant was a mature and responsible adult of approximately 60 years of age when he abused his position of trust and accessed the private files of 18 people. Each time he knowingly accessed private files, he placed his own desires above the government's need for reliable and trustworthy conduct. His rationale that he wished to discover who had supplied false child-support information, and that his ex-wife had lied

about his support payments, does not justify his actions. He failed to disclose his behavior until the SCI investigation forced him to do so.

Applicant wore military medals that he purchased at flea markets, and held himself out as a man who had earned them. Violation of 18 U.S.C. § 704 is not alleged in this case; however, the fact that wearing unearned military decorations has been defined by Congress as improper for decades indicates the gravity of this falsehood. The two decades that Applicant maintained his false boasts about being in combat in Vietnam raises concerns about his credibility and judgment.

Finally, the fact that Applicant's untrustworthy conduct occurred while he held a security clearance is most troubling. He was aware of the obligations placed on those who hold security clearances, but that knowledge was not enough to prevent him from engaging in untrustworthy behavior to satisfy his own desires.

Overall, the record evidence fails to satisfy the doubts raised about Applicant's suitability for a security clearance. For all these reasons, I conclude Applicant has not mitigated the security concerns arising from the cited adjudicative guideline.

Formal Findings

Paragraph 1, Guideline M	AGAINST APPLICANT
Subparagraph 1.a.	Against Applicant
Paragraph 2, Guideline E	AGAINST APPLICANT
Subparagraphs 2.a. – 2.d.	Against Applicant
Subparagraph 2.e. ¹⁰	For Applicant

Conclusion

In light of all of the circumstances presented by the record in this case, it is not clearly consistent with the national interest to allow Applicant access to classified information. Applicant's request for a security clearance is denied.

RITA C. O'BRIEN
Administrative Judge

¹⁰ The information stated in SOR allegation 2.e. is not disqualifying conduct under the Directive.