



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



In the matter of:	)	
	)	
XXXXXXXXXX, XXXX	)	ISCR Case No. 06-09643
SSN: XXX-XX-XXXX	)	
	)	
Applicant for Security Clearance	)	

**Appearances**

For Government: Braden M. Murphy, Esq., Department Counsel  
For Applicant: *Pro Se*

April 30, 2009

**Decision**

TUIDER, Robert J., Administrative Judge:

Applicant failed to mitigate security concerns regarding Guidelines J (Criminal Conduct), M (Use of Information Technology Systems), and E (Personal Conduct). Clearance is denied.

**Statement of the Case**

On August 22, 2003, Applicant submitted a Security Clearance Application, Standard Form (SF) 86.<sup>1</sup> On November 20, 2008, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) to her, pursuant to Executive Order 10865, *Safeguarding Classified Information Within Industry*, dated February 20, 1960, as amended and modified, and Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (Directive), dated January 2,

<sup>1</sup> The August 2003 security clearance application is the most recent one in Applicant's file. He filled it out in connection with a previous employer and was terminated from that employer in July 2005. Applicant is sponsored for a security clearance by his current employer.

1992, as amended, modified and revised.<sup>2</sup> The SOR alleges security concerns under Guidelines J (Criminal Conduct), M (Use of Information Technology Systems), and E (Personal Conduct). The SOR detailed reasons why DOHA could not make the preliminary affirmative finding under the Directive that it is clearly consistent with the national interest to grant or continue a security clearance for her, and recommended referral to an administrative judge to determine whether a clearance should be granted, continued, denied, or revoked.

On November 26, 2008, Applicant responded to the SOR allegations, and elected to have his case decided on the written record in lieu of a hearing. A complete copy of the file of relevant material (FORM), dated January 7, 2009, was provided to him, and he was afforded an opportunity to file objections and submit material in refutation, extenuation, or mitigation.<sup>3</sup> Applicant did not submit any information within the 30-day time period after receiving a copy of the FORM. The case was assigned to me on April 16, 2009.

### **Findings of Fact**

Applicant admitted all of the SOR allegations. His admissions are incorporated herein as findings of fact. I make the following additional findings of fact:

Applicant is a 33-year-old defense contractor employee. The FORM did not contain any information regarding his education background. Applicant did serve in the U.S. Navy from August 1993 to September 2002, and was discharged as an E-4. He held a secret security clearance while in the Navy. Applicant has been married since April 2004. Although the FORM makes references to children and stepchildren, it does not contain specific information about them.<sup>4</sup>

Applicant's background investigation included a review of his SF-86,<sup>5</sup> and various documents pertaining to his past arrests, and the underlying basis surrounding his discharge from his previous employer.<sup>6</sup> The Government established by Applicant's

---

<sup>2</sup>On Aug. 30, 2006, the Under Secretary of Defense (Intelligence) published a memorandum directing application of revised Adjudicative Guidelines to all adjudications and other determinations made under the Directive and Department of Defense (DoD) Regulation 5200.2-R, Personnel Security Program (Regulation), dated Jan. 1987, as amended, in which the SOR was issued on or after Sep. 1, 2006. The revised Adjudicative Guidelines are applicable to Applicant's case.

<sup>3</sup> DOHA transmittal letter is dated January 9, 2009; and Applicant received the FORM on January 30, 2009. The DOHA transmittal letter informed Applicant that he had 30 days after Applicant's receipt to submit information.

<sup>4</sup> Item 4.

<sup>5</sup> Item 3.

<sup>6</sup> Items 4 – 11.

admissions and evidence presented that Applicant committed four criminal offenses, all of which he admits. Applicant has two arrests and convictions for Driving under the Influence (DUI) of Alcohol in April 1996 and May 1998. In February 2003, he was convicted of providing alcohol to a minor after two of his teenage stepchildren and their friends consumed beer at his house. In September 2004, he was convicted of misdemeanor assault for slapping his teenage stepdaughter in the face.

Applicant was employed by a defense contractor from May 2003 to July 2005, and was involuntarily terminated for violating his employer's internet and e-mail policies, which he admitted. His employer undertook this action after having given him two written warnings in February 2004 and October 2004 informing him that he risked termination unless he altered his course of conduct.

His termination for violating his employer's internet and e-mail policies was cross-alleged under personal conduct. (SOR ¶ 3.a.). Also, when Applicant completed his August 2003 SF-86, he failed to list the full extent of his alcohol/drug offenses. In particular, he failed to list his February 2003 charge of contributing alcohol to minor and subsequent conviction of providing alcohol to a minor. He also failed to list his May 1998 arrest and charge of driving under the influence. A closer reading of Applicant's August 2003 SF-86 reveals that Applicant did, in fact, disclose his 2003 offense elsewhere on his SF-86. Applicant does not dispute that he deliberately failed to list his 1998 DUI.

Applicant offered no mitigating evidence.

### **Policies**

When evaluating an Applicant's suitability for a security clearance, the Administrative Judge must consider the revised adjudicative guidelines (AG). In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially disqualifying conditions and mitigating conditions, which are useful 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, these guidelines are applied in conjunction with the factors listed in the adjudicative process. The Administrative Judge's over-arching adjudicative goal is a fair, impartial and common sense 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. Likewise, I have avoided drawing inferences grounded on mere speculation or conjecture.

In the decision-making process, the Government has the initial burden of establishing controverted facts alleged in the SOR by “substantial evidence,”<sup>7</sup> demonstrating, in accordance with the Directive, that it is not clearly consistent with the national interest to grant or continue an applicant’s access to classified information. Once the Government has produced substantial evidence of a disqualifying condition, the burden shifts to Applicant to produce evidence “to rebut, explain, extenuate, or mitigate facts admitted by applicant or proven by Department Counsel, and [applicant] has the ultimate burden of persuasion as to obtaining a favorable clearance decision.” Directive ¶ E3.1.15. The burden of disproving a mitigating condition never shifts to the Government. See ISCR Case No. 02-31154 at 5 (App. Bd. Sep. 22, 2005).<sup>8</sup>

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 protect or safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation as to potential, rather than actual, risk of compromise of classified information.

Section 7 of Executive Order 10865 provides that 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* Executive Order 12968 (Aug. 2, 1995), Section 3.

## **Analysis**

### **Guideline J, Criminal Conduct**

Under Guideline J, the Government’s concern is:

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. AG ¶ 30.

---

<sup>7</sup> See Directive ¶ E3.1.14. “Substantial evidence [is] such relevant evidence as a reasonable mind might accept as adequate to support a conclusion in light of all the contrary evidence in the record.” ISCR Case No. 04-11463 at 2 (App. Bd. Aug. 4, 2006) (citing Directive ¶ E3.1.32.1). “This is something less than the weight of the evidence, and the possibility of drawing two inconsistent conclusions from the evidence does not prevent [a Judge’s] finding from being supported by substantial evidence.” *Consolo v. Federal Maritime Comm’n*, 383 U.S. 607, 620 (1966). “Substantial evidence” is “more than a scintilla but less than a preponderance.” See *v. Washington Metro. Area Transit Auth.*, 36 F.3d 375, 380 (4<sup>th</sup> Cir. 1994).

<sup>8</sup> “The Administrative Judge [considers] the record evidence as a whole, both favorable and unfavorable, evaluate[s] Applicant’s past and current circumstances in light of pertinent provisions of the Directive, and decide[s] whether Applicant ha[s] met his burden of persuasion under Directive ¶ E3.1.15.” ISCR Case No. 04-10340 at 2 (App. Bd. July 6, 2006).

Under Guideline J, there are two Disqualifying Conditions raised by Applicant's conduct: AG ¶ 31(a) "a single serious crime or multiple lesser offenses;" and AG ¶ 31(c) "allegation or admission of criminal conduct, regardless of whether the person was formally charged, formally prosecuted, or convicted." The Government established these Disqualifying Conditions through Applicant's admissions and evidence presented.

There are four Mitigating Conditions under Guideline J that potentially apply: AG ¶ 32(a) "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(b) "the person was pressured or coerced into committing the act and those pressures are no longer present in the person's life;" AG ¶ 32(c) "evidence that the person did not commit the offense;" and AG ¶ 32(d) "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, of constructive community involvement."

Applicant admitted each offense as alleged in the SOR under this concern, but offered no mitigating explanations. As such, I am unable to apply any of the potential Mitigating Conditions under Guideline J.

### **Guideline M (Use of Information Technology Systems)**

Under Guideline M, the Government's concern is:

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, manipulation, storage, or protection of information. AG ¶ 39.

Under Guideline M, there is one Disqualifying Condition raised by Applicant's conduct: AG ¶ 40(e) "unauthorized use of a government or other information technology system." The Government established this Disqualifying Condition through Applicant's admissions and evidence presented.

There are three Mitigation Conditions under Guideline M that potentially apply: AG ¶ 41(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;" AG ¶ 41(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 AG ¶ 41(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's unauthorized internet and e-mail use was intentional, repeated, and came after warnings from his supervisor to cease and desist, under threat of termination. Applicant's employer considered his actions serious enough to warrant his termination, so that his actions cannot be considered "minor." Applicant has not shown that the security concerns raised by his actions can be viewed as mitigated.

### **Guideline E (Personal Conduct)**

Under Guideline E, the Government's concern is:

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 ¶ 15.

Under Guideline E, there are several Disqualifying Conditions raised by Applicant's conduct. Applicant's unauthorized internet and e-mail use at a previous employer (discussed under Guideline M) is cross-alleged as a separate concern under Personal Conduct because it constitutes questionable judgment and unwillingness to comply with rules and regulations warranting application of AG ¶ 16(d) "credible adverse information that is not explicitly covered under any other guideline and may not be sufficient by itself for an adverse determination, but which, when combined with all available information 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. This includes but is not limited to consideration of: . . . (3) a pattern of dishonesty or rule violations."

The remaining Guideline E allegation concerns a falsification concern that warrants application of AG ¶ 16(e): "deliberate omission, concealment, or falsification of relevant facts from any personnel security questionnaire, personal history statement, or similar form used to conduct investigations, determine employment qualifications, award benefits or status, determine security clearance eligibility or trustworthiness, or award fiduciary responsibilities.

Considering the record as a whole, I am convinced Applicant deliberately failed to disclose the information. Numerous factors weighed in my analysis to reach that conclusion, including: Applicant's age, his level of education, his employment history, and his admission.

There are five Mitigating Conditions under Guideline E that potentially apply: AG ¶ 17(a) "the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts;" AG ¶ 17(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;" 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;" 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;" and AG ¶ 17(e) "the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress."

Applicant admitted each offense as alleged in the SOR under this concern, but offered no mitigating explanations. His behavior raises questions about his ability and willingness to follow the law, and ultimately, to protect classified information. His falsification and lack of candor weigh against a finding of rehabilitation and positive behavioral changes. As such, I am unable to apply any of the potential Mitigating Conditions under Guideline E.

Additionally, for the same reasons outlined under the discussions of Guidelines J, M and E, incorporated herein, I conclude Applicant's behavior shows questionable judgment, lack of reliability, and untrustworthiness.

To conclude, Applicant presented little or no evidence to explain, extenuate, or mitigate the security concerns raised. Applicant did not meet his ultimate burden of persuasion to obtain a favorable clearance decision. In reaching this conclusion, the whole person concept was given due consideration, and that analysis does not support a favorable decision.

I take this position based on the law, as set forth in *Department of Navy v. Egan*, 484 U.S. 518 (1988), my "careful consideration of the whole person factors"<sup>9</sup> and supporting evidence, my application of the pertinent factors under the Adjudicative Process, and my interpretation of my responsibilities under the Guidelines. Applicant has mitigated or overcome the Government's case. For the reasons stated, I conclude he is not eligible for access to classified information.

---

<sup>9</sup> See ISCR Case No. 04-06242 at 2 (App. Bd. June 28, 2006).

### **Formal Findings**

Formal findings for or against Applicant 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 J: Subparagraphs 1.a. – 1.d.:	AGAINST APPLICANT Against Applicant
Paragraph 2, Guideline M: Subparagraph 2.a.:	AGAINST APPLICANT Against Applicant
Paragraph 3, Guideline E: Subparagraph 3.a. – 3.b.:	AGAINST APPLICANT Against Applicant

### **Conclusion**

In light of all of the circumstances presented by the record in this case, it is not clearly consistent with national security to grant Applicant eligibility for a security clearance. Clearance is denied.

---

ROBERT J. TUIDER  
Administrative Judge