DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 17-02666
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Charles C. Hale, Esq., Department Counsel
For Applicant: *Pro se*

04/18/2018

Decision

HEINTZELMAN, Caroline E., Administrative Judge:

Applicant failed to mitigate security concerns raised under Guideline E (Personal Conduct). As the Facility Security Officer (FSO), he failed to report key management personnel's criminal behavior and provided misleading statements to a Government investigator. Eligibility for access to classified information is denied.

History of the Case

Applicant submitted a security clearance application (SCA) on August 1, 2016. On August 15, 2017, the Department of Defense (DOD) sent him a Statement of Reasons (SOR) alleging security concerns under Guideline E (Personal Conduct). The DOD acted under Executive Order (EO) 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) promulgated in Security Executive Agent Directive 4, *National Security Adjudicative Guidelines* (December 10, 2016), for all decisions on or after June 8, 2017.

Applicant answered the SOR on August 21, 2017, and requested a decision on the record without a hearing. On September 26, 2017, a complete copy of the File of

Relevant Material (FORM), containing eight Items, was mailed to Applicant and received by him on October 4, 2017. The FORM notified Applicant that he had an opportunity to file objections and submit material in refutation, extenuation, or mitigation within 30 days of his receipt of the FORM. Applicant did not object to the Government's Items. Hence, Items 1 through 8 are admitted into evidence without objection. He did not submit a response to the FORM. The case was assigned to me on March 1, 2018.

Findings of Fact

Applicant admitted all three allegations in the SOR with explanations. His admissions are incorporated into my findings of fact.

Applicant is a 65-year-old director of contracts at a closely-held-family business. He has worked for this defense contractor since July 1976, and requires a security clearance for his employment. Applicant served as his employer's FSO for approximately 20 years until February 2015 (Item 7). He has held a security clearance since approximately 1989 (Item 3 at 25). He graduated from high school in 1970 and served in the State A's National Guard from October 1970 until December 1976, when he was honorably discharged. Applicant has been married to his second wife since 1976 and has one child from each of his marriages (Item 3).

In August 2014, the president and majority shareholder (Individual A) of Applicant's employer (Company A), a family-owned business, pled guilty to illegally diverting corporate funds for himself. The Department of Justice found Individual A's illegal behavior occurred between 2008 and 2011. Individual A fraudulently converted over $900,000 from his company to himself. He also failed to pay almost $285,000 in federal taxes on this fraudulently obtained money. Company A manufactures parts for the defense and aerospace industries (Item 6).

On December 11, 2014, an industrial security specialist (ISR) conducted a security vulnerability assessment (SVA) on Company A. During the investigation, it was discovered that multiple significant adverse information reports were not reported by Applicant through the joint personnel adjudicative system (JPAS). One of these reports included significant adverse information regarding Individual A. As the FSO, Applicant was responsible for filing a report in JPAS regarding Individual A when he became aware of this information.[1] The Defense Security Service (DSS) was not informed of this issue involving Individual A until the ISR conducted the SVA. DSS determined this information is especially significant because "it directly affects [Company A's] ability to maintain a Facility Clearance (FCL)" (Item 7).

[1] The National Industrial Security Program Operating Manual (NISPOM) states "Contractors are required to report certain events that: impact the status of the facility clearance (FCL); impact the status of an employee's personnel security clearance (PCL); may indicate the employee poses an insider threat; affect proper safeguarding of classified information, or that indicate classified information has been lost or compromised" (Item 5).

On December 17, 2014, the DSS sent a culpability report to the Department of Defense Consolidated Adjudication Facility (DODCAF) for Applicant based upon the information addressed above (Item 7 at 1). On February 4, 2015, DDS suspended Applicant's security clearance (Item 7 at 2). This report notes Applicant's failure to report multiple significant adverse information reports was gross negligence (Item 7).[2]

In May 2017, Applicant told the Government investigator he was unaware of Individual A's criminal behavior until it became public knowledge in August 2014 (Item 4 at 2). He initially told the investigator that his failure to report Individual A's criminal behavior and subsequent conviction in JPAS was due to a computer issue, which prevented him from accessing JPAS. He also asserted he tried to call the facility inspector, but was unable to reach him. Upon further questioning by the Government investigator, Applicant admitted he did not report this information in a timely manner because Individual A's father (Individual B), the owner of Company A, asked Applicant not to make an adverse information report (AIR), to protect Company A and his son. Applicant did not file the AIR due to a sense of loyalty to Company A and Individual B (Item 4 at 2).

In his Answer to the SOR, Applicant provided emails between himself and the ISR regarding JPAS. Applicant's first email to the ISR was sent on December 22, 2014, after DSS initiated an investigation regarding his behavior (Item 2).

Policies

"[N]o one has a 'right' to a security clearance."[3] 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."[4] 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."[5]

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 and reliable information about the person, past and present, favorable and unfavorable.

---

[2] DSS found Applicant should have be familiar with proper reporting requirements as he had been an FSO in the NISP for over 20 years (Item 7).

[3] *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988).

[4] *Egan* at 527.

[5] EO 10865 § 2.

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 that 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."[6] 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.[7] "Substantial evidence" is "more than a scintilla but less than a preponderance."[8] The guidelines presume a nexus or rational connection between proven conduct under any of the criteria listed therein and an applicant's security suitability.[9] Once the Government establishes a disqualifying condition by substantial evidence, the burden shifts to the applicant to rebut, explain, extenuate, or mitigate the facts.[10] An applicant has the burden of proving a mitigating condition, and the burden of disproving it never shifts to the Government.[11]

An applicant "has the ultimate burden of demonstrating that it is clearly consistent with the national interest to grant or continue his security clearance."[12] "[S]ecurity clearance determinations should err, if they must, on the side of denials."[13]

---

[6] EO 10865 § 7.

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

[8] *See v. Washington Metro. Area Transit Auth.*, 36 F.3d 375, 380 (4th Cir. 1994).

[9] ISCR Case No. 92-1106 at 3, 1993 WL 545051 at *3 (App. Bd. Oct. 7, 1993).

[10] Directive ¶ E3.1.15.

[11] ISCR Case No. 02-31154 at 5 (App. Bd. Sep. 22, 2005).

[12] ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002).

[13] *Egan*, 484 U.S. at 531; *See also* AG ¶ 2(b).

Analysis

Guideline E: Personal Conduct

AG ¶ 15 expresses the security concern pertaining to 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 or sensitive information. Of special interest is any failure to cooperate or provide truthful and candid answers during national security investigative or adjudicative processes. The following will normally result in an unfavorable national security eligibility determination, security clearance action, or cancellation of further processing for national security eligibility:
>
> > (a) refusal, or failure without reasonable cause, to undergo or cooperate with security processing, including but not limited to meeting with a security investigator for subject interview, completing security forms or releases, cooperation with medical or psychological evaluation, or polygraph examination, if authorized and required; and
> >
> > (b) refusal to provide full, frank, and truthful answers to lawful questions of investigators, security officials, or other official representatives in connection with a personnel security or trustworthiness determination.

AG ¶ 16 describes three conditions that could raise a security concern and be disqualifying in this case:

> (a) deliberate omission, concealment, or falsification of relevant facts from an personnel security questionnaire, personal history statement, or similar form used to conduct investigations, determine employment qualifications, award benefits or status, determine national security eligibility or trustworthiness, or award fiduciary responsibilities;
>
> (b) deliberately providing false or misleading information; or concealing or omitting information, concerning relevant facts to an employer, investigator, security official, competent medical or mental health professional involved in making a recommendation relevant to a national security eligibility determination, or other official government representative; and
>
> (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 individual may not properly safeguard classified or sensitive information.

Applicant's failure to report Individual A's criminal behavior in JPAS and his failure to be honest and forthright with the Government investigator establishes the above disqualifying conditions.

After the Government raised potentially disqualifying conditions, the burden shifted to Applicant to rebut or prove mitigation of the resulting security concerns. AG ¶ 17 provides two conditions that could mitigate security concerns in this case:

(a) the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts; and

(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.

Applicant failed to report significant adverse information regarding Individual A. When he was confronted regarding his failure, he provided misleading and false information to a Government investigator. He ultimately admitted the truth behind his failure to report the adverse information, but only after he was confronted. AG ¶ 23(a) does not apply. Applicant held a security clearance for approximately 26 years and served as Company A's FSO for 20 years. His behavior was not minor as DSS described it as "gross negligence." Applicant violated the responsibility entrusted in him by the DOD when he put his loyalty to Company A and Individual B above his loyalty to the U.S. Government. AG ¶ 23(c) does not apply.

Whole-Person Concept

Under AG ¶ 2(c), the ultimate determination of whether the granting or continuing of national security eligibility is clearly consistent with the interests of national security must be an overall common sense judgment based upon careful consideration of the following guidelines, each of which is to be evaluated in the context of the whole person. An administrative judge should consider the nine adjudicative process factors listed at AG ¶ 2(d):

(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 Guideline E in my whole-person analysis, and I have considered the factors in AG ¶ 2(d). After weighing the disqualifying and mitigating conditions under Guideline E, and evaluating all the evidence in the context of the whole person, I conclude that Applicant has not mitigated the personal conduct concerns raised by his behavior. Accordingly, Applicant has not carried his burden of showing that it is clearly consistent with the national security interests of the United States to grant him eligibility for access to classified information.

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, Personal Conduct:	AGAINST APPLICANT
Subparagraphs 1.a. – 1.c.:	Against Applicant

Conclusion

I conclude that it is not clearly consistent with the national security interests of the United States to continue Applicant's eligibility for access to classified information. Clearance is denied.

_____
Caroline E. Heintzelman
Administrative Judge