DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 16-04051
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Daniel F. Crowley, Department Counsel
For Applicant*: Pro se*

January 26, 2018

_____

Decision

_____

LOKEY ANDERSON, Darlene D., Administrative Judge:

Statement of the Case

On December 21, 2015, Applicant submitted a security clearance application (e-QIP). On March 13, 2017, the Department of Defense issued a Statement of Reasons (SOR) to Applicant detailing security concerns under Guideline E, Personal Conduct. The action was taken 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) effective September 1, 2006.

Applicant answered the SOR on April 5, 2017. He requested that his case be decided by an administrative judge on the written record without a hearing. (Item 2.) On June 29, 2017, Department Counsel submitted the Government's written case. A complete copy of the File of Relevant Material (FORM), containing 6 Items, was mailed to Applicant and received by him on July 12, 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 failed to respond to the FORM. Applicant did not object to Items 1 through 6, and they were admitted into evidence.

The SOR in this case was issued under the adjudicative guidelines that came into effect within the DoD on September 1, 2006. Security Executive Agent Directive (SEAD) 4, *National Security Adjudicative Guidelines*, implements new adjudicative guidelines, effective June 8, 2017. All national security eligibility decisions issued on or after June 8, 2017, are to be decided using the new *National Security Adjudicative Guidelines for Determining Eligibility for Access to Classified Information or Eligibility to Hold a Sensitive Position* (AG), as implemented by SEAD 4. I considered the previous adjudicative guidelines, effective September 1, 2006, as well as the new AG, effective June 8, 2017, in adjudicating Applicant's national security eligibility. My decision would be the same under either set of guidelines, although this decision is issued pursuant to the new AG.

Findings of Fact

Applicant is 59 years old. He is the owner and consultant of a defense contracting company. He is seeking to obtain a security clearance in connection with his employment in the defense industry.

Paragraph 1 (Guideline E – Personal Conduct) The Government alleged that Applicant is ineligible for a clearance because his conduct exhibits questionable judgement, lack of candor, dishonesty or unwillingness to comply with rules and regulations that 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 answer during the security clearance process or any other failure to cooperate with the security clearance process.

From January 2012 to October 2012, Applicant was employed as the Chief Operating Officer (COO) for Company A that provided technologies and software design to customize and enhance the Microsoft SharePoint platform. Company A was headquartered in the United States. Applicant worked at the headquarters, and there were offices in Vietnam and the Netherlands. (Government Exhibits 4 and 5.)

The Applicant, as COO, arranged for the Company A to hire his brother to head the Office in when it opened in 2006. The office in Vietnam was established as a development office only, meaning there were no sales emanating from that office. In 2006, Applicant's brother was hired as the Chief Representative for the Vietnam office. Applicant's brother reported to Applicant and was responsible for all aspects of the operations as the company's representative in Vietnam. Applicant's responsibilities from headquarters included receiving and approving all funding requests from his brother in Vietnam. From the time Applicant's brother started working with the company until he resigned in 2012, there were numerous unexplained increases in expenses for

the Vietnam Office, yet there were no receipts or other documentation available to support the expenses because the documents were lost in an officer renovation. As the result of an audit, it was determined that the company paid the Vietnam office approximately $478,836 in cash, for various things that were not support by sufficient documentation. It was also determined that the Applicant had used the Company A's corporate credit card on multiple occasions to purchase personal items worth several thousands of dollars. (Government Exhibits 4 and 5.)

In October 2012, it was determined that Applicant and his brother started doing business as Company B in direct competition with Company A, while they were both still employed by Company A, and while still holding their respective positions as Chief Operating Officer and Chief Representative. It was also alleged that Applicant and his brother, while still employed with Company A, notified several Company A employees of a business opportunity in Vietnam worth approximately 16 million dollars. Applicant and his brother resigned from Company A in October 2012. Both the Applicant and his brother are currently still employed with Company B. (Government Exhibits 4 and 5.)

There is evidence that after leaving Company A, Applicant and his brother continued to participate in a scheme to take Company A's entire team of SharePoint programmers and developers and relocate them the Company B, their new business created for the purpose of taking Company A's resources and using them to compete against Company A. Malicious and false rumors were spread among Company A employees suggesting to them that Company A would be going out of business in a few months. Thus, encouraging them to leave Company A and go work for Company B. Several employees from Company A have accepted Applicant's invitation to work for Company B. (Government Exhibit 5.)

In 2013, Company A filed a lawsuit against the Applicant and his brother in civil court alleging misappropriation of trade secrets, breach of fiduciary duty, statutory business conspiracy, conversion, and tortious interference with contracts. In September 2014, Applicant signed a settlement agreement wherein he agreed that he and his brother and their company were in possession of data belonging to Company A, and that Company A claimed was confidential and a trade secret. Applicant agreed to pay Company A exactly $100,000 to settle the matter. (Government Exhibit 6.)

A letter dated March 3, 2016, from Applicant's counsel indicates that Applicant only settled the lawsuit filed against him by Company A as a business decision to avoid the cost he would incur in litigation fees. He argues that the claims were never proven and that there was a complete lack of evidence to support them. He claims that Applicant denies the validity of any of the claims.

Policies

When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the adjudicative guidelines (AG). In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially

disqualifying conditions and mitigating conditions, which are to be used 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, administrative judges apply the guidelines in conjunction with the factors listed in AG ¶ 2(a) describing the adjudicative process. The administrative judge's overarching adjudicative goal is a fair, impartial, and commonsense 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 the 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.

Under Directive ¶ E3.1.14, the government must present evidence to establish controverted facts alleged in the SOR. Under Directive ¶ E3.1.15, the applicant is responsible for presenting "witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by the applicant or proven by Department Counsel." The applicant has the ultimate burden of persuasion to obtain a favorable clearance decision.

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 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 EO 10865 provides that adverse 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* EO 12968, Section 3.1(b) (listing multiple prerequisites for access to classified or sensitive information).

Analysis

Guideline E, Personal Conduct

The security concern relating to the guideline for Personal Conduct is set out in AG ¶ 15:

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 disqualifying conditions are potentially applicable:

(a) 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;

(b) deliberately providing false or misleading information concerning relevant facts to an employer, investigator, security official, competent medical authority, or other official government representative;

(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

(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:

(1) untrustworthy or unreliable behavior to include breach of client confidentiality, release of proprietary information, unauthorized release of sensitive corporate other government protected information;

(2) disruptive, violent, or other inappropriate behavior in the workplace;

(3) a pattern of dishonesty or rule violations;

(4) evidence of significant misuse of Government or other employer's time or resources.

(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, or (2) while in another country, engaging in any activity that is illegal in that country or that is legal in that country but illegal in the United States and may serve as a basis for exploitation or pressure by the foreign security or intelligence service or other group.

(f) violation of a written or recorded commitment made by the individual to the employer as a condition of employment; and

(g) association with persons involved in criminal activity.

Applicant's behavior, when considered as a whole, demonstrates that there has been questionable conduct and at least a misappropriation of trade secrets. It is noted that the matter was not litigated but instead settled, and so it is not proven whether the other claims were valid. However, Applicant agreed to pay Company A $100,000 to settle all disputes and claims against him. The settlement agreement clearly states that Company B is in possession of data belonging to Company A, and that Company A claims that the data is confidential and trade secret. The settlement agreement also specifically requires Applicant and company B to destroy any data belonging to Company A, with certain restrictions. Based upon the statement of facts set forth above, the above disqualifying conditions have been established.

AG ¶ 17 provides conditions that could mitigate security concerns. None of the mitigating conditions are applicable here.

(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;

(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

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

Applicant's involvement in such a scheme demonstrates untrustworthy, poor judgment and unreliability. There is nothing in the record to guarantee that this situation would not occur again, given the right set of facts.

Whole-Person Concept

Under the whole-person concept, the 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. The 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.

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.

I considered the potentially disqualifying and mitigating conditions in light of all relevant facts and circumstances surrounding this case. Applicant's profile is not that of a person with whom the Government would have great trust. Applicant's questionable judgment is disqualifying and does not show the requisite good judgment and reliability required to have access to sensitive and/or classified information. Overall, the record evidence leaves me with many questions and doubts as to Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude Applicant has not mitigated the Personal Conduct concerns.

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 E:	AGAINST APPLICANT
Subparagraph 1.a:	Against 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 grant or continue Applicant's eligibility for a security clearance. Eligibility for access to classified information is denied.

Darlene Lokey Anderson
Administrative Judge