DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
REDACTED	)	ISCR Case No. 14-00996
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Alison O'Connell, Esq., Department Counsel
For Applicant: Jessica Carmichael, Esq.
Kel McClanahan, Esq.

03/19/2015

Decision

MENDEZ, Francisco, Administrative Judge:

Applicant failed to mitigate the personal conduct security concerns. He kept without permission a computer-based application that he developed for his former employer. He previously stated during security interviews and on his security clearance application that the application contained the personally identifiable information (PII) of thousands of individuals, but at hearing recanted his earlier admissions. Applicant's past conduct and inconsistent statements about his conduct continue to raise doubts about his current reliability and trustworthiness. Clearance is denied.

Statement of the Case

On June 2, 2014, the Department of Defense (DOD), in accordance with DOD Directive 5220.6, as amended (Directive), issued Applicant a Statement of Reasons (SOR), alleging security concerns under Guideline E (Personal Conduct). Applicant answered the SOR and requested a hearing.

On December 18, 2014, the hearing was held. Government Exhibits (Gx.) 1 – 4 and Applicant's Exhibits (Ax.) 1 – 7 were admitted into evidence.[1] Applicant testified and called his current and past supervisor, as well as his neighbor, as witnesses. He also submitted and, over Department Counsel's objection, I accepted for administrative notice DOD Regulation 5400.11, *DOD Privacy Program*, dated May 14, 2007. The hearing transcript (Tr.) was received on January 6, 2015.

Motion to Amend SOR

Department Counsel moved to amend SOR ¶ 1.d to reflect that Applicant falsified his security clearance application (SCA) by failing to disclose that he left Company A under unfavorable circumstances (vice, as originally alleged, that he was terminated). Hearing Exhibit (Hx.) I. Applicant did not object to the amendment and maintains that he was not terminated by Company A, nor left under unfavorable circumstances. Hx. II. I granted the motion.

Findings of Fact

After a thorough review of the pleadings, transcript, and exhibits, I make the following findings of fact:[2]

Applicant is in his early fifties and has earned several advanced academic degrees. He has worked as a federal contractor since 2001, and held a security clearance since 2002. He worked for Company A between 2001 and 2006. (Tr. at 64, 139-140; Gx. 1; Gx. 3) He received permission from his former employer to download software to his home computer to allow him to work from home. He also downloaded without permission other employer-provided commercial software to enhance his ability to support his government client. (Tr. at 91-93, 129-132)

In 2005, while employed by Company A, Applicant developed an application for his government client to better manage their workforce. The client decided to go in another direction and the human resources application (HR application) was never fully developed. Applicant kept the HR application because it contained coding he had written that he believed could potentially be useful on future projects. He did not get Company A or the government client's permission to keep the HR application. (Tr. at 64-78)

[1] Applicant objected to the admission of Gx. 3, which contains a Report of Investigation (ROI), on several evidentiary grounds. I overruled the objection (Tr. at 26-29), and also determined that the exhibit did not violate the Directive's prohibition against the admission of an ROI without authentication. The ROI in this case was not prepared by DOD, but by another government agency. Directive, ¶¶ E.3.1.19 – E.3.1.20. *See generally*, ISCR Case No. 11-12461 (App. Bd. Mar. 14, 2013); ISCR Case No. 10-08390 (App. Bd. Mar. 30, 2012) *See also*, *Palmieri v. United States*, *et. al*., No. 12-1403, 2014 U.S. Dist. LEXIS 155613, at *24-*33 (D.C. Dist. Ct. Nov. 3, 2014) (admission of a letter from a DOD criminal investigative agency in a security clearance hearing did not violate either the Directive or appellant's due process rights)

[2] In reaching my findings of fact, I have made only those inferences reasonably supported by the evidence and, where necessary, resolved any potential conflict raised by the evidence.

Applicant testified that others in the information technology (IT) field routinely keep code they develop for use on future projects and to share with other developers without first getting approval from their employer or the government. (Tr. at 151-152). His current supervisor, who has worked in the government IT field for about 30 years, testified that Applicant's conduct in downloading software without permission and retaining the HR application without first getting approval would be considered "minor infractions at best." (Tr. at 44)

In 2006, Applicant left Company A because his employer was no longer able to pay him the six-figure salary he was receiving. The company had submitted a low offer to successfully fend off a competitor's bid for the government contract Applicant was working on. After Company A succeeded in retaining the contract, Applicant's salary was reduced by nearly half. Applicant left Company A after someone else was selected for the lead project position and receiving a six-figure salary offer from Company B. (Tr. at 78-83, 86-91, 127-129, 140-144, 154-156; Ax. 2)

Applicant listed his employment with Company A on his current SCA. He reported that his reason for leaving Company A was for a "better offer, better pay." (Gx. 1 at 14) Government interviews of Company A's vice president and former supervisor that were done close in time to when Applicant left Company A corroborate Applicant's version of events leading to his resignation. The witnesses described Applicant as an excellent employee. (Gx. 3, ROI at 1, 9-11) His last performance appraisal from Company A reflects that he consistently exceeded expectations in all areas. (Ax. 3) The appraisal specifically notes that the government customer rated Applicant and his team as being "truly outstanding." (Ax. 3 at 4) The appraisal further states that the government customer was "looking for an expanded role for [Company A] due to [Applicant's] performance and leadership." (Ax. 3 at 5)

In 2007, Applicant's application for access to sensitive compartmented information (SCI) was denied by another government agency (AGA) due to his personal conduct and misuse of IT systems. The AGA found, in part, that while employed by Company A, Applicant downloaded software without permission and kept the HR application without approval. Additionally, the AGA noted that during interviews with government agents, Applicant stated that the HR application contained the PII of the government client's workforce – some 13,000 individuals. (Gx. 3, *Decision Statement*)

Following the interviews with government agents in 2007, Applicant deleted all copies of the HR application, including one that was saved on his Company B work computer. At hearing, Applicant described his state of mind during those interviews and averred the statements that he made regarding the HR application containing PII was a result of the harsh interrogation techniques employed by the agents. Also after the interview with the government agents, Applicant contacted his former client to seek permission to keep the HR application. He deleted copies of the application even before hearing back from the client because one of the agents "harangued" him about his conduct. (Tr. at 148) Applicant was eventually informed by his former client that Company A did not give permission for his possession of the application.

Applicant disclosed the denial to SCI access by the AGA on his current SCA, which he submitted in June 2012. In explaining the denial, Applicant wrote that the HR application "may have contained [PII], or it may have been test data." (Gx. 1 at 35) At hearing, Applicant testified that the HR application only contained dummy or test data, not PII. He explained that at the early development stage he was at with the application he would not have had access to actual PII. He likely used the names of the individuals he was working with at the time and inputted fictitious information in the PII fields. He also stated that, for technological reasons, he could not have saved the HR application if it actually contained the PII of 13,000 individuals on a CD or other portable device. (Tr. at 64-78, 99-127, 132-138, 144-150)

Applicant has worked for his current employer since 2009. He has successfully completed and routinely receives refresher training on the proper handling and safeguarding of sensitive information, to include PII. He seeks permission from the proper officials before sharing or keeping any IT applications or matters that he works on or develops. He is highly regarded by his current and former supervisors, co-workers, and neighbors for his trustworthiness, reliability, and good judgment. (Tr. at 34-58, 74-76, 94-98; Gx. 3, ROI at 1, 9-11; Ax. 1; Ax. 6; Ax. 7)

Applicant has not been involved in any misuse of IT systems beyond those matters that led to the denial of his request for SCI access in 2007. In addition to changes to his work environment and the manner in which he handles sensitive information, Applicant testified about the major changes in his personal life. Notably, Applicant is now married and has two young children. He is dedicated to his family, having traded in the Hummer that he once drove as a bachelor for the minivan that he now drives as the father of young children. (Tr. at 93-94)

Policies

"[N]o one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988). Individual applicants are only eligible for access to classified information "only upon a finding that it is clearly consistent with the national interest" to authorize such access. E.O. 10865 § 2.

When evaluating an applicant's eligibility, an administrative judge must consider the adjudicative guidelines. In addition to brief introductory explanations, the guidelines list potentially disqualifying and mitigating conditions. The guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, an administrative judge applies the guidelines in a common sense manner, considering all available and reliable information, in arriving at a fair and impartial decision.

The Government must present evidence to establish controverted facts alleged in the SOR. Directive ¶ E3.1.14. On the other hand, an 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." Directive ¶ E3.1.15. An applicant has the ultimate burden of persuasion to establish their eligibility.

In resolving the ultimate question regarding an applicant's eligibility, an administrative judge must resolve "[a]ny doubt concerning personnel being considered for access to classified information . . . in favor of national security." AG ¶ 2(b). Moreover, "security clearance determinations should err, if they must, on the side of denials." *Egan*, 484 U.S. at 531.[3] However, a judge must decide each case based on its own merits because there is no *per se* rule requiring disqualification.[4]

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. 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 an applicant may deliberately or inadvertently fail to safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation of 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." E.O. 10865 § 7. Thus, a decision to deny a security clearance amounts to a finding that an applicant, at the time the decision was rendered, did not meet the strict guidelines established for determining eligibility for access to classified information.

Analysis

Guideline E, Personal Conduct

The personal conduct security concern is explained at 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.

The SOR alleges that Applicant falsified his SCA by failing to disclose he left Company A under unfavorable circumstances. If proven by substantial evidence, such conduct raises the Guideline E concern and the disqualifying condition listed at AG ¶ 16(a).[5] Applicant refuted the falsification allegation. He was not fired by Company A, nor

[3] *See also*, ISCR Case No. 07-16511 at 3 (App. Bd. Dec. 4, 2009) ("Once a concern arises regarding an Applicant's security clearance eligibility, there is a strong presumption against the grant or maintenance of a security clearance.").

[4] ISCR Case No. 11-12202 at 5 (App. Bd. June 23, 2014).

[5] Deliberate omission, concealment, or falsification of relevant facts from any personnel security questionnaire . . . or similar form used to . . . determine security clearance eligibility.

left under unfavorable circumstances. Instead, the record evidence established that Applicant left Company A for the reason he listed on his SCA, to wit: "better offer, better pay." (Gx. 1 at 14)[6] Accordingly, SOR ¶ 1.d is decided in Applicant's favor.

Applicant's questionable judgment in downloading software and retaining the HR application without his former employer's approval also raise the personal conduct security concern. His conduct implicates the following disqualifying conditions:

> AG ¶ 16(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
>
> AG ¶ 16(f): violation of a written or recorded commitment made by the individual to the employer as a condition of employment.[7]

Applicant submitted substantial evidence that would tend to indicate reform and rehabilitation, to include the passage of time without a repeat of the underlying conduct at issue. Such favorable evidence would generally mitigate the personal conduct security concerns.[8] However, Applicant's testimony was in direct conflict with the statements he previously made to government investigators and during the current security clearance investigation as to whether the HR application contained PII.[9] His

[6] The falsification allegation was based upon two short sentences that *only* appear in the summary section of the 25-page ROI, specifically, that Applicant was "dismissed" by Company A because he "was not responsive and was conducting personal business during billable time." (Gx. 3, ROI at 1). The ROI does not contain information as to where the agent who prepared the summary received the unfavorable information, and the AGA did not even credit this purported adverse employment information as a basis for denial to SCI access. Company A's vice president notes that any reported unfavorable information regarding Applicant's work performance was provided by those with a motive to fabricate. Moreover, the substantive portions of the ROI contain significant information, notably the interviews of Applicant's former supervisor and Company A's vice president, that fully corroborate Applicant's stated reasons for leaving Company A. (Gx. 3, ROI at 1, 9-11) Applicant also submitted contemporaneous e-mails and documentation that further corroborate his assertion that he did not leave Company A under unfavorable circumstances, but instead for a better offer and better pay. (Ax. 2)

[7] Although the Government did not submit evidence of a specific workplace rule, regulation, or agreement that Applicant violated, the evidence established that his conduct was proscribed by his former employer. Furthermore, Applicant's witness described the conduct as constituting minor infractions. ISCR Case No. 11-05079 (App. Bd. June 6, 2012) (violation of a specific rule or regulation is unnecessary when an applicant's conduct clearly raises security concerns).

[8] *See generally* AG ¶ 17(c). Applicant did mitigate concerns raised by the allegations in SOR ¶¶ 1.b and 1.c. He has not downloaded software without authority in over 10 years and fully disclosed his conduct to his former employer after the interviews with the government agents in 2007.

[9] Even if I were to credit Applicant's assertion that the statement he made to government investigators regarding the HR application containing PII was the result of a coercive or an overly intimidating

inconsistency on such a material point undercuts the favorable evidence of rehabilitation and reform, and raises continuing concerns about his reliability and trustworthiness.[10] Accordingly, none of the personal conduct mitigating conditions apply.

Whole-Person Concept

Under the whole-person concept, an administrative judge must evaluate an applicant's eligibility for a security clearance by considering the totality of an applicant's conduct and all the relevant circumstances. An administrative judge should consider the nine factors listed at AG ¶ 2(a).[11] I hereby incorporate my above comments and highlight some additional whole-person factors. Applicant has worked for the government as a contractor for 14 years. By all accounts, his work has been exceptional. However, his past conduct in keeping without permission an application he developed for his former employer and the inconsistent statements he has made regarding whether the application contained PII raise continuing concerns about his reliability and trustworthiness. Overall, doubts persist about Applicant's continued eligibility for access to classified information.[12]

Formal Findings

I make the following formal findings regarding the allegations in the SOR:

Paragraph 1, Guideline E (Personal Conduct):	AGAINST APPLICANT
Subparagraph 1.a:	Against Applicant
Subparagraphs 1.b – 1.d:	For Applicant

interrogation, such does not explain why five years later in a non-coercive environment he voluntarily stated on his SCA that the HR application may have contained PII. At the same time, I do not find that he took the HR application for personal pecuniary interest or other improper motive. *Contrast with*, ISCR Case No. 14-00963 (App. Bd. Jan. 13, 2015).

[10] ISCR Case No. 14-00952 at 4 (Mar. 13, 2015) ("To the extent an applicant has presented ambiguous or contradictory testimony, it is not consistent with the ultimate burden for the Judge to construe inconsistencies in an applicant's favor."). *See also*, ISCR Case No. 99-0228 at 6, 2001 DOHA LEXIS 58, *17 ("Given Applicant's inability or unwillingness to recognize or acknowledge that his conduct was improper and wrong, there is nothing mitigating about the passage of time...").

[11] The non-exhaustive list of adjudicative 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.

[12] ISCR Case No. 11-00391 at 3 (App. Bd. Dec. 1, 2011) ("The Directive requires a Judge to resolve any doubt in favor of national security.").

Conclusion

In light of the record evidence and for the foregoing reasons, it is not clearly consistent with the national interest to grant Applicant continued access to classified information. Applicant's request for a security clearance is denied.

_____
Francisco Mendez
Administrative Judge