DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 12-00276
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Robert J. Kilmartin, Esq., Department Counsel
For Applicant: *Pro se*

06/30/2014

_____

Decision

_____

DUFFY, James F., Administrative Judge:

Applicant failed to mitigate the personal conduct security concerns. Eligibility for access to classified information is denied.

Statement of the Case

On September 17, 2011, Applicant submitted an Electronic Questionnaire for Investigations Processing (e-QIP). On March 7, 2014, the Department of Defense Consolidated Adjudications Facility (DOD CAF) issued Applicant a Statement of Reasons (SOR) detailing security concerns under Guideline E (personal conduct). DOD CAF took that action 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) implemented on September 1, 2006.

On April 6, 2014, Applicant answered the SOR and requested a hearing. The case was assigned to me on May 1, 2014. The Defense Office of Hearings and Appeals (DOHA) issued a notice of hearing on May 1, 2014. The hearing was convened as scheduled on May 20, 2014. At the hearing, Department Counsel offered Government's Exhibits (GE) 1 through 5. Applicant testified and offered Applicant's Exhibits (AE) A through E. The record was left open until June 3, 2014, to provide Applicant an opportunity to submit additional matters. Applicant timely submitted documents that were marked as AE F through AA. Applicant objected to GE 3, a redacted military police investigation, and his objection was overruled. The remaining proffered exhibits were admitted into evidence without objection. DOHA received the hearing transcript (Tr.) on June 4, 2014.

Findings of Facts

Applicant is a 45-year-old engineering administrative support employee of a defense contractor. He has worked for that contractor since July 2011. He graduated from high school in 1986 and earned an associate's degree in about 1991. He served on active duty in the U.S. Air Force from October 1986 to January 2010 and retired honorably in the grade of technical sergeant (E-6). He first married in 1992 and divorced in 1999. He married his current wife in 2004. He has three children between the ages of eight and eighteen. He has held a security clearance since about 1986.[1]

The SOR listed five Guideline E allegations asserting that Applicant hacked into an email account, recorded another's proprietary documents onto a compact disc (CD), stole government furniture, and was awarded nonjudicial punishment for theft of military property and for a crime against intellectual property in 2009 (SOR ¶ 1.a); that he falsified his e-QIP dated September 17, 2011, by failing to report he received nonjudicial punishment for crimes against intellectual property (SOR ¶ 1.b); that he falsified the e-QIP by failing to report an arrest and charge for driving under the influence of alcohol (DUI) in February 2004 (SOR 1.c); that he falsified the e-QIP by failing to report that he entered into an information technology system and removed media without authorization (SOR ¶ 1.d); and that he falsified material facts during an interview with an investigator by failing to report information about hacking into an email account, recording of another's proprietary information on a CD, and being awarded nonjudicial punishment for a crime against intellectual property (SOR ¶ 1.e). In his Answer to the SOR, Applicant denied all of the SOR allegations.[2]

From about August 2008 to January 2009, Applicant's wife worked as a receptionist at a business (Company X) that assisted individuals with immigration issues, such as the submission of requests for work visas. Applicant was never

[1] Tr. at 5-6, 74; GE 1.

[2] Applicant Answer to the SOR.

employed at Company X but did assist the company and its chief executive officer (CEO) with their computer problems while his wife worked there.[3]

In late 2008, Applicant's wife became dissatisfied working at Company X. Applicant and his wife decided to start their own company that would provide the same type of immigration services. In January 2009, Applicant incorporated that business (Company Y) in his name. Applicant's wife and another Company X employee who was knowledgeable about immigration laws and procedures came to work for Company Y.[4]

In June 2009, the CEO of Company X alleged that Applicant may have used government computers to hack into Company X's computers. The CEO further alleged that Applicant rerouted his emails, which included communications from federal agencies, without his authorization to Applicant's company. As a result of those allegations, a military police investigation was initiated.[5]

The military police investigation revealed that Applicant hacked into the CEO's email account, rerouted the CEO's emails without authorization to his account, and took government furniture from an aircraft hangar for use at Company Y. Applicant admitted to engaging in that conduct. Applicant claimed that he hacked into the CEO's email to observe its content as a means of protecting his family from the CEO's threats and that he thought the government furniture was being thrown away. The government furniture that Applicant took consisted of a desk, ladder, microwave, and other items.[6]

The military police investigation also indicated that Applicant confessed to recording Company X proprietary information onto a CD and taking that information. However, the written statement that Applicant provided to investigators is difficult to read and confusing. At the hearing, Applicant denied copying proprietary information from Company X onto a CD. He stated that he advised an employee of Company Y on how to copy information from a computer onto a flash drive, but claimed that copying of information occurred at Company Y, not Company X. On the other hand, the report of the military police investigation indicated that a CD was uncovered that contained proprietary information from Company X, including a list of its clients. This CD was labeled "Immigration Stuff [Company X]" in a handwriting style that investigators opined was extremely similar to Applicant's.[7]

[3] Tr. at 33-42, 49-51, 66-68; GE 3, 5.

[4] Tr. at 33-42; GE 3, 5.

[5] GE 3.

[6] Tr. at 42-44, 47-53, 69-71; GE 3, 5. In his Answer to the SOR, Applicant indicated that he used the CEO's password to enter the CEO's email account without authorization. He knew the CEO's password from working on the CEO's computer.

[7] Tr. at 28-42, 47-53, 66-68; GE 3 (¶ 2-44), 5.

In October 2009, Applicant was awarded nonjudicial punishment for theft of military property worth $500 or less and for a crime against intellectual property by taking data belonging to another without authorization in violation of a state law. His punishment consisted of a suspended reduction to staff sergeant (E-5), forfeiture of $1,414 pay per month for two months, and a reprimand. Applicant did not appeal the punishment. His security clearance was suspended for a period of time as a result of the investigation, but was later reinstated. In the present hearing, Applicant testified that he thought the crime against intellectual property pertained to his hacking into the CEO's email account.[8]

Applicant submitted an e-QIP on September 17, 2011. In Section 15d of that document, he was asked if he had been subjected to a court-martial or any other disciplinary proceeding under the Uniform Code of Military Justice, including nonjudicial punishment, in the last seven years. He responded "Yes" to that question and indicated that he received Article 15 punishment for "removed property less than $500" in October 2009. He explained that the property in question was a set of desks that he assumed was junk and would be discarded, but later learned those items were slated for disposal through official channels. His response to that e-QIP question did not mention the "crimes against intellectual property" charge or his hacking into the CEO's email account.[9]

In Section 22e of the e-QIP, Applicant was asked if he had ever been charged with any offenses related to alcohol or drugs. He answered "No" to that question and failed to report that he was arrested and charged with DUI on February 1, 2004, after he crashed his vehicle multiple times.[10]

In Sections 27a and 27c of the e-QIP, Applicant was asked if he had illegally or without proper authorization entered into any information technology system and if he removed media from an information technology system without authorization when prohibited by rules, guidelines, and regulations. He responded "No" to both of those questions and failed to disclose his hacking into the CEO's email account and rerouting the CEO's emails to his account.[11]

At the hearing, Applicant claimed that his failure to disclose on the e-QIP any information about the crime against intellectual property offense on the e-QIP was an oversight. He stated that he had no intent to deceive by excluding that information. He noted that, at the time he submitted the e-QIP, he had financial problems and was focused on those problems and other matters more than the prior nonjudicial punishment. Regarding his failure to report information about his DUI arrest on the

[8] Tr. at 50-53, 68-72, 78-79; GE 2, 4.

[9] Tr. at 26-60; GE 1.

[10] Tr. at 44-47, 64-66, 71-72; GE 1.

[11] GE 1.

e-QIP, Applicant stated that he thought he had to report such matters only if it occurred in the last seven years. Finally, he indicated that his failure to report the computer hacking incident in Section 27 of the e-QIP was also an oversight. He stated that he had no reason to conceal such matter because the government had access to the military police report regarding those offenses.[12]

Applicant was interviewed by an Office of Personnel Management (OPM) investigator on October 14, 2011. During the interview, Applicant provided details of the theft of government furniture from an on-base hangar and the awarding of nonjudicial punishment for that offense. The summary of the OPM interview contained no mention of Applicant being charged with a "crime against intellectual property" offense or his hacking into the CEO's email account. In his testimony at the hearing, he indicated that he was never asked about the hacking incident during the interview.[13]

Applicant presented documents showing that the CEO of Company X was disbarred from the practice of law in one state and subjected to disciplinary action by other state bar associations. He was later convicted of attempted murder and sentenced to 30 years in jail. He was also convicted of racketeering and practicing law without a license for which he was sentenced to 80 months in prison that ran concurrently with his 30-year sentence. The racketeering charge arose from his operation of Company X.[14]

Applicant was awarded the Air Force Achievement Medal and Air Force Commendation Medal. He presented enlisted performance evaluations that showed that he was a top performer. He also submitted character reference letters from supervisors, coworkers, military members, and friends that describe him as dependable, trustworthy, and reliable. He is active in the community and in his church.[15]

Policies

When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the adjudicative guidelines. 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 the adjudicative process. The administrative judge's overarching adjudicative goal is a fair, impartial, and commonsense decision. According

[12] Tr. at 53-63, 71-77; GE 1.

[13] Tr. at 61-63; GE 3.

[14] Tr. at 66-67, 69-72; AE A-C.

[15] AE F-AA.

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.

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 security 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 of 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 for personal conduct is set out in AG ¶ 15, as follows:

> 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;
>
> (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 evidence 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 or 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; 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 2009, Applicant was awarded nonjudicial punishment for stealing government property and for a crime against intellectual property by taking data belonging to another without authorization in violation of a state law. In this regard, he admitted that he stole government furniture, hacked into the email account of the CEO of Company X, and forwarded the CEO's emails to his computer. Despite Applicant's denials, substantial

evidence was presented to show that Applicant took proprietary information from Company X. AG ¶¶ 16(c), 16(d) and 16(e) apply to SOR ¶ 1.a.

When Applicant submitted his e-QIP, he disclosed in response to Section 15d that he received nonjudicial punishment, but failed to indicate the offenses at that proceeding included a crime against intellectual property. He also failed to disclose in Sections 27a and 27c of the e-QIP that he hacked into the email account of the CEO of Company X and forwarded the CEO's emails to his computer. His claim that he failed to disclose information on his e-QIP about the crime against intellectual property due to an oversight is not believable. Substantial evidence was presented to establish that Applicant intentionally concealed information on his e-QIP. AG ¶ 16(a) applies to SOR ¶¶ 1.b and 1.d.

Applicant claim that he failed to disclose information about his 2004 DUI because he thought that information only needed to be disclosed if it occurred in the last seven years is plausible. I find in favor of Applicant on SOR ¶ 1.c.

During an OPM interview, Applicant discussed being awarded nonjudicial punishment for theft of government property. The summary of the interview makes no mention of being awarded punishment for the crime against intellectual property. Applicant claimed that he was not asked about the crime against intellectual property during the interview. Because we do not know what questions Applicant was asked during the interview, insufficient evidence was submitted to establish that he provided false information during that interview. AG ¶ 16(b) does not apply. I find in favor of Applicant on SOR ¶ 1.e.

AG ¶ 17 provides conditions that could mitigate security concerns. The following are potentially applicable:

> (a) the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts;
>
> (b) the refusal or failure to cooperate, omission, or concealment was caused or significantly contributed to by improper or inadequate advise of unauthorized 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 information, the individual cooperated fully and truthfully;
>
> (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;
>
> (e) the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress; and
>
> (f) the information was unsubstantiated or from a source of questionable reliability.

Applicant stole government property, hacked into another's email account, and rerouted another's email to his account. He also deliberately failed to disclose information on an e-QIP. His misconduct is recent and demonstrates a lack of honesty, trustworthiness, and good judgment. After examining all of the applicable mitigating conditions, I find that none apply.

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. I have incorporated my comments under Guideline E in my whole-person analysis. Some of the factors in AG ¶ 2(a) were addressed under that guideline, but some warrant additional comment.

Applicant served in the Air Force for about 23 years and retired honorably as a technical sergeant. Since retiring, he has continued to serve the Federal Government by working for a defense contractor. He is a valued employee and thought highly of by coworkers and friends. Nevertheless, his questionable conduct continues to raise serious questions about his reliability, trustworthiness, and good judgment. He has failed to present sufficient evidence to conclude such wrongdoing is unlikely to recur.

Overall, the record evidence leaves me with questions and doubts about Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude Applicant has not mitigated the personal conduct security concerns.

Formal Findings

Formal findings 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
Subparagraphs 2.a – 2.b:	Against Applicant
Subparagraph 2.c:	For Applicant
Subparagraph 2.d:	Against Applicant
Subparagraph 2.e:	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 grant Applicant eligibility for a security clearance. Eligibility for access to classified information is denied.

_____
James F. Duffy
Administrative Judge