DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 13-00603
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Jeff A. Nagel, Esq., Department Counsel
For Applicant: *Pro se*

May 6, 2014

_____

Decision

_____

GOLDSTEIN, Jennifer I., Administrative Judge:

Security concerns are raised under the Guideline for Personal Conduct because Applicant made intentionally false statements to an investigative agent. Additionally, Applicant was terminated by three different employers for misconduct. Applicant failed to mitigate the Personal Conduct concerns. Eligibility for access to classified information is denied.

Statement of the Case

Applicant submitted her Electronic Questionnaires for Investigations Processing (e-QIP) on September 20, 2011. On July 29, 2013, the Department of Defense issued a Statement of Reasons (SOR) to Applicant detailing security concerns under the guideline for Financial Considerations. 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 after September 1, 2006.

Applicant answered the SOR (Answer) in an undated submission received by the Defense Office of Hearings and Appeals (DOHA) on October 9, 2013, and requested an administrative determination be made without a hearing. On February 19, 2014, Department Counsel issued Applicant an Amendment to the SOR (ASOR), which withdrew all of the allegations under Guideline F, Financial Considerations, and replaced them with new security concerns under Guideline E, Personal Conduct. Department Counsel requested a hearing in this matter by letter dated February 20, 2014. Applicant answered the ASOR on March 24, 2014. The case was assigned to me on March 3, 2014. A notice of hearing was issued to Applicant on March 4, 2014, scheduling a hearing for March 26, 2014. On March 26, 2014, the hearing convened as scheduled. The Government offered the ASOR. Applicant had no objection to the ASOR, and the amendment was granted.

The Government presented Exhibits (GE) 1 and 2, which were admitted without objection. Applicant testified on her own behalf, and offered Applicant's Exhibits (AE) A through G, which were admitted into the record without objection. Applicant requested that the record be left open to allow her to submit additional evidence and her request was granted. Applicant presented an additional exhibit, marked AE H. Department Counsel had no objection to AE H, and it was admitted into the record. DOHA received the transcript of the hearing (Tr.) on April 3, 2014. The record closed on April 28, 2014.

Findings of Fact

Applicant is 35 years old. She is divorced and has one minor child. She passed the General Education Development (GED) test, but did not graduate from high school. She attended some college classes, but did not earn a degree. She is a self-educated cyber security expert. She has worked in the field of cyber security since at least 2001. She currently is the managing member and founder of a cyber-security firm. She seeks a security clearance in connection with that firm. She hopes to procure defense contracts. (GE 1; Tr. 42, 47-49.)

The Government alleged that Applicant is ineligible for a clearance because she engaged in conduct involving questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations. The ASOR alleged nine subparagraphs (1.a through 1.i) under Guideline E. Applicant admitted ASOR subparagraphs 1.b, 1.c, 1.g, 1.h, and 1.i. Applicant denied subparagraphs 1.a, 1.d, 1.e, and 1.f.

Applicant's employment was terminated by four different employers between 2001 and 2009. Her employment in 2001 was terminated for publishing a vulnerability finding she generated for her employer, as alleged in ASOR subparagraph 1.i. She explained that she tested a technology for security vulnerabilities at the instruction of her employer. After she discovered vulnerabilities, she prepared a report. The manufacturer of the technology was not taking action to patch the identified vulnerabilities. She testified that her supervisor requested that she publish the vulnerability finding, but she produced no documentation to support her claim that her supervisor instructed her to publish the report. She published the findings online in a

public forum, and her employment was terminated as a result. She explained in her testimony that she "serve[s] two masters"; she had a duty to the vendor of the technology, but she also had to "serve other fellow security engineers" by alerting them to the problem. She acknowledged that by publishing her findings, she also put people at risk of being hacked until patches were created to fix the vulnerabilities, because publishing the findings made hackers aware of the existence of vulnerabilities. (GE 1; GE 2; AE A; Tr. 60-75.)

Applicant's employment was terminated in April 2004 for misuse of equipment and company information, as alleged in ASOR subparagraph 1.h. Applicant testified that while working for this employer, she started her own company in the evenings. She thought that the software she developed in her outside company could be helpful to her employer, so she prepared a PowerPoint presentation and used both her employer's logo and her own company's logo together in the presentation. About a year after preparing the presentation, a human resources officer from her employer approached her with a printout of the PowerPoint slides. Applicant claims she was accused of falsely telling people that her employer was a client of her outside business. Her employment was terminated as a result of the allegations. (GE 1; GE 2; Tr. 76-80.)

In December 2004 Applicant's employment with another employer was terminated for taking excessive sick leave, as alleged in ASOR subparagraph 1.g. She had only worked for that employer for three months and was in a probationary period of employment. She caught the flu and missed two weeks of work. (GE 1; GE 2; Tr. 80-81.)

In June 2009 Applicant was terminated from a fourth employer (Company 4) for requesting personal user information regarding a customer, as alleged in ASOR subparagraph 1.a through 1.c. Applicant contended that she was a paid confidential informant for a U.S. intelligence agency, outside of her employment with her employer. She was researching a subject for the intelligence agency and by coincidence, discovered that the subject was Company 4's customer. She instant messaged her supervisor and requested personal information on the user. She did not attempt to obtain the information through hacking into her Company 4's computer system or through other illicit means. The day after she requested the user information her employment was terminated for "conflict of interest." (GE 1; GE 2; AE A; Tr. 81-106.)

Applicant explained that her job terminations were not her fault, but occurred because she possessed leadership qualities. She sees herself as an entrepreneur who has successfully created several companies. (Tr. 44-45.)

Applicant completed an e-QIP on September 20, 2011. On her e-QIP she disclosed that at the time she was working for Company 4, she "was also working as part of a special program with a US Intelligence Agency," as alleged in ASOR subparagraph 1.e. She failed to further identify that intelligence agency elsewhere on her e-QIP. When asked about this statement by an investigator for the U.S. Office of Personnel Management, Applicant explained she "did not list it as employment as it was undercover and classified," as alleged in ASOR subparagraph1.f. She disclosed to the

investigator only that she was a paid undercover informant for an intelligence agency and was tracking a target that she discovered was using her employer's site, as alleged in subparagraph 1.d. On May 29, 2013, she authenticated the report of investigation that contained the assertion that she could not list this employment on her e-QIP because it was undercover and classified, without any additions or deletions.

At the hearing, Applicant admitted she never previously possessed a security clearance and that the information about her role as a confidential informant with an intelligence agency was not classified. She claims she signed a non-disclosure or confidentiality agreement and did not believe she was permitted to discuss the details of her activities with the intelligence agency with "anyone, including within the U.S. Intelligence Community or law enforcement." She did not recall "using the term classified" with the agent. In her post-hearing submission, she provided emails she received from an agent purportedly with the intelligence agency in connection with her work. She identified the agency in her cover letter. She did not provide a copy of a non-disclosure agreement. She testified that she worked for the agency from 2007 to 2009. She was paid cash for her services and she did not disclose the payments on her income tax returns. (GE 1; GE 2; AE A; AE H; Tr. 51, 81-106.)

Applicant is an articulate and intelligent cyber-security expert. She has an impressive resume and has worked in high-level positions of trust. She presented several endorsements that indicate she is known for her creativity and intelligence. According to one letter of recommendation, she has "a strong sense of integrity and commitment to purpose." (AE B; AE C; AE D; AE E; AE F; AE G.)

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 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 national security." In reaching the 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. The 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 for the Personal Conduct guideline 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; 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 combine 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 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.

Applicant identified her work as a confidential informant with an intelligence agency on her e-QIP in explaining her termination from Company 4. While she did not list the name of that agency, I find that her disclosure shows she intentionally put the Government on notice of her activities and that she did not intentionally omit or falsify her e-QIP. However, when she was asked about her involvement with that intelligence agency, she told the investigator she did not list it as employment as it was undercover and classified. She adopted her statement to the investigator in May 2013 in her answer to interrogatories, and did not alter her explanation. She later admitted that she has never held a security clearance and the information about her role as a confidential informant was not classified. She deliberately provided false or misleading information concerning her role with the intelligence agency to the investigator. AG ¶ 16(a) is inapplicable, but ¶ 16(b) applies.

Applicant's employment was terminated by four different employers between 2001 and 2009. While her termination due to illness cannot be said to be a case of poor judgment on Applicant's part, the remaining three terminations were directly attributable to her poor judgment. Additionally, her publication of vulnerability findings was a breach of client confidentiality. Applicant acknowledged that she has a strong entrepreneurial spirit and that as a cyber-security expert, she sometimes serves two masters. That entrepreneurial drive has created conflicts between her employer's policies and her ethics. Her decisions, which resulted in three terminations, support a whole-person

assessment that she may continue to exercise questionable judgment, untrustworthiness, unreliability, lack of candor, and unwillingness to comply with rules and regulations; and therefore may not properly safeguard protected information. AG ¶ 16(c) applies.

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 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;
>
> (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.

After considering the mitigating conditions outlined above in AG ¶ 17, none of them were established in this case. Applicant did not make prompt or good-faith efforts to correct her falsification or concealment. She provided no information that indicates she was ill-advised on the security clearance process. Falsifying material information is a serious offense and Applicant has done nothing to show that similar lapses in judgment are unlikely to recur. Further, she failed to take responsibility for her actions and continued to assert that she played no role in her terminations from three companies. She has not provided sufficient evidence to meet her burden of proof for her personal conduct.

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 the 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 pertinent facts and circumstances surrounding this case. I have incorporated my comments under E in my whole-person analysis. Some of the factors in AG ¶ 2(a) were addressed under those guidelines, but some warrant additional comment.

Applicant is a talented and dedicated cyber-security expert. She is well respected by her customers and those that wrote letters of support on her behalf. She was terminated from three different employers for misconduct and made false statements to an investigative agent. She failed to establish that future misconduct would be unlikely. Overall, the record evidence leaves me with serious 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 security 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
Subparagraph 1.b:	For Applicant
Subparagraph 1.c:	Against Applicant
Subparagraph 1.d:	For Applicant
Subparagraph 1.e:	For Applicant
Subparagraph 1.f:	Against Applicant
Subparagraph 1.g:	For Applicant
Subparagraph 1.h:	Against Applicant
Subparagraph 1.i:	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.

_____
Jennifer I. Goldstein
Administrative Judge