DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 17-02144
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Nicole A Smith, Esq., Department Counsel
For Applicant: Pro Se
02/22/2019

_____

Decision

_____

KILMARTIN, Robert J., Administrative Judge:

Applicant did not mitigate the security concerns under Guideline M (use of information technology) and Guideline E (personal conduct). Applicant's eligibility for access to classified information is denied.

Statement of the Case

Applicant submitted a security clearance application (SCA) on June 4, 2014. On August 11, 2017, the Department of Defense Consolidated Adjudications Facility (DOD CAF) issued Applicant a Statement of Reasons (SOR) detailing security concerns under Guideline M, use of information technology and Guideline E, personal conduct. The DOD CAF acted under Executive Order (EO) 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; DOD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the adjudicative guidelines (AGs) implemented by DOD on June 8, 2017.

Applicant provided a four-page response to the SOR on September 1, 2017, denying all of the SOR allegations and including a two-page typed explanation of events. Applicant also requested a hearing before an administrative judge. The case was assigned to me on August 3, 2018. On December 3, 2018, the Defense Office of Hearings and Appeals

(DOHA) notified Applicant that the hearing was scheduled for December 20, 2018. I convened the hearing as scheduled.

Government Exhibits (GE) 1 – 4 were admitted into evidence without objection. I left the record open until January 15, 2019, for Department Counsel and Applicant to provide any post-hearing documents. On January 10, 2019, Applicant provided an e-mail with three attachments: the court disposition from his step-son's incident; a recent Questionnaire for Public Trust Position (SF-85); and a recent Declaration for Federal Employment. These were marked as Applicant's Exhibits (AE) A–C respectively and admitted without objection. Department Counsel asked to leave the record open for an additional week and I granted her request over Applicant's objection. An e-mail chain marked Hearing Exhibit (HE) 1 reflects the back-and-forth colloquy. At the hearing, Applicant testified on his own behalf, but submitted no documentation. DOHA received the transcript (Tr.) on January 4, 2019.

Findings of Fact[1]

Applicant is 50 years old. He obtained a bachelor's degree in 1991 and a master's degree in 2002. (Tr. 10-12) Applicant was married in 1992, divorced in 2006, and he remarried in 2009. He reports two children and two stepchildren from his wife's first marriage. He previously served as a police officer in a small town from 1995 to 2002. Applicant has been employed as an information technology (IT) professional by a federal contractor since September 2015. Applicant reports no military service, and he has held a security clearance since 2006. (Tr. 18-20)

SOR ¶ 1.a alleges under Guideline M that in 2015, Applicant violated his employer's information protection acceptable-use policy by viewing child-pornography images on his company's laptop computer. A second allegation at SOR ¶ 2.a asserts that Applicant was terminated from his employment on August 20, 2015, as a result. SOR ¶ 2.b alleges that Applicant failed to disclose this derogatory information during an interview on December 19, 2016, with an authorized investigator for DOD. SOR ¶ 2.c cross-alleges the same misconduct under SOR ¶ 1.a and raises a concern under Guideline E, personal conduct. The basis for these allegations is an August 19, 2015 letter of termination from the vice president of his company (GE 4), and Applicant's answers to interrogatories dated July 31, 2017, with an attached two-page statement clarifying the summary of his personal subject interview (PSI) conducted by an authorized investigator on December 19, 2016 (GE 3).

Applicant was terminated from his employment by a previous federal contractor on August 19, 2015. (Tr. 21) He testified that he was called in by his supervisors in June 2015, and told that inappropriate images had been found on his work laptop computer. Applicant admitted he had viewed adult pornography on this laptop. They took his laptop away and provided him with another loaner laptop. (Tr. 34) Applicant was called in again on August 19, 2015. He vehemently denied ever downloading, accessing, or viewing child pornography-images on his work laptop computer. (Tr. 45) He did not ever see the offensive

[1] Unless stated otherwise, the source of the information in this section is Applicant's June 4, 2014 security clearance application (SCA) (GE 1).

images obtained by his employer, but was told that his laptop contained inappropriate images. He was terminated after 13 ½ years with that employer, and he did not appeal. (Tr. 45) Applicant had taken computer-security courses and training and he knew that the company prohibited viewing adult pornography on work computers. (Tr. 50, 83)

Applicant lived with his wife and four children in 2015. Local police obtained and executed a search warrant at his house in March 2016 seeking evidence of a computer crime. (Tr. 36) Since the internet service provider (ISP) subscription at that address was in Applicant's name, he was interviewed first by the police. He vehemently denied viewing or downloading child-pornography images on his laptop computer. When Applicant's 17-year-old stepson was interviewed separately, he admitted downloading the compressed files of pornographic images of his minor girlfriend on his computer. (Tr. 39, AE A) The stepson went to court and pled guilty to a reduced charge of computer harassment. He was sentenced to two years of probation and therapy, which he completed, and the conviction was expunged. (Tr. 40-41) Applicant never gave anybody else his password or computer access card (CAC) card to access his work laptop computer. (Tr. 43)

In a December 19, 2016, personal subject interview (PSI), a clearance interviewer went through the various sections of Applicant's June 2014 SCA and asked Applicant questions. Applicant told her that he voluntarily resigned from his employment in 2015 because he did not like the contract. (Tr. 56) Applicant testified that this was a snap decision and he lied to her because he was embarrassed. Applicant wholeheartedly regrets this and the ensuing falsifications in sections 13 (c) (employment record) and 27 (use of information technology systems) of the same SCA. (Tr. 57) Applicant was not forthcoming with the clearance interviewer about derogatory information in his background. Applicant testified that he viewed adult pornography on his work laptop for three years starting in 2012, and he last viewed adult pornography in 2015. (Tr. 77, 81)

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, the adjudicative guidelines list potentially disqualifying conditions and mitigating conditions, which are 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, these guidelines are applied 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 to AG ¶ 2(a), the adjudicative process is an examination of a sufficient period and a careful weighing of a number of variables of an individual's life to make an affirmative determination that the individual is an acceptable security risk. This is 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 national security eligibility 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, an "applicant is responsible for presenting witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by applicant or proven by Department Counsel, and has the ultimate burden of persuasion as to obtaining 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 that an 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.

Analysis

Guideline M, Use of Information Technology

> The Concern. Failure to comply with rules, procedures, guidelines, or regulations pertaining to information technology systems may raise security concerns about an individual's reliability and trustworthiness, calling into question the willingness or ability to properly protect sensitive systems, networks, and information. Information Technology includes any computer-based, mobile, or wireless device used to create, store, access, process, manipulate, protect, or move information. This includes any component, whether integrated into a larger system or not, such as hardware, software, or firmware, used to enable or facilitate these operations.[2]

In assessing Applicant's case, I considered the following pertinent disqualifying conditions in AG ¶ 40:

> (e) unauthorized use of any information technology system; and
>
> (f) introduction, removal, or duplication of hardware, firmware, software, or media to or from any information technology system when prohibited by rules, procedures, guidelines, or regulations or when otherwise not authorized.

[2] AG ¶ 39.

Applicant has admitted in his response to the SOR that he improperly downloaded pornography onto his work computer without authorization and in violation of his employer's IT policy. This meets the government's burden in establishing application of the above-mentioned disqualifying conditions, and shifts the focus to potentially mitigating conditions.

AG ¶ 41(a) could potentially mitigate the use of information technology concerns:

> so much time has elapsed since the behavior happened, or it happened under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment.

Applicant viewed pornographic images on his work laptop computer for three years from 2012 to 2015. Applicant testified credibly that he has refrained from this behavior for almost four years. He is contrite and he has been punished by this former employer when he was terminated and unemployed for a period. However, he was not forthcoming with the clearance interviewer about the termination. He told her he voluntarily resigned because he did not like the contract. He repeatedly violated his employer's IT policy by viewing the pornography. Under the circumstances, I am not convinced that this violation and lapse in judgment won't recur in the future.

Guideline E, Personal Conduct

.

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

> The Concern. 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. . . .

AG ¶ 16 describes conditions that could raise a security concern and may be disqualifying. The following disqualifying conditions are potentially applicable:

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

I find that the evidence and testimony presented, implicate AG ¶¶ 16 (b) and 16 (f). Applicant acknowledges having computer training with the company and being

aware of his company's zero-tolerance policy for downloading pornography on company computers, and he admits to violating it. Moreover, Applicant was terminated by his employer for this behavior. He exacerbated matters by failing to disclose the truth about his termination from his employer in 2015 to the clearance investigator.

Conditions under AG ¶ 17 that could potentially mitigate security concerns include:

> (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 contributed to 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.

My analysis under adjudicative guideline M above, is the same under this this administrative guideline E and is herein incorporated by reference. Applicant lied to the clearance investigator in December 2016 about his termination. He has not been candid and forthright throughout the security clearance process. Insufficient time has passed to conclude that his misconduct in viewing pornography and his falsifications to the investigator occurred under unique circumstances and are not likely to recur. Applicant has taken positive steps to acknowledge his mistakes, and he no longer views pornography but he has not had counseling. The mitigating conditions above do not 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 the circumstances. The 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.

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 the facts and circumstances surrounding this case. I have incorporated my comments under Guidelines M and E in my whole-person analysis. Some of the factors in AG ¶ 2(d) were addressed under those guidelines. Notably, Applicant has a demonstrated record of over 20 years of service in law enforcement and as a federal contractor with a security clearance. He is a father of two children and two stepchildren. Most importantly, Applicant deliberately deceived the clearance investigator about his reason for leaving employment in 2015. He has not met his burden of persuasion.

There is sufficient evidence to conclude that Applicant has violated the company's rules, regulations, policies or procedures pertaining to use of IT, and that he lied about it to the investigator. He has not met his burden of persuasion. I am not convinced that these were isolated incidents. The record evidence leaves me with questions and doubts as to Applicant's suitability for a security clearance. For all these reasons, I conclude Applicant has not mitigated the security concerns arising under Guidelines M and E.

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 M:	AGAINST APPLICANT
Subparagraph 1.a:	Against Applicant
Paragraph 2, Guideline E:	AGAINST APPLICANT
Subparagraphs 2.a – 2.c:	Against Applicant

Conclusion

In light of all of the circumstances presented by the record in this case, it is not clearly consistent with the interests of national security to grant Applicant a security clearance. Eligibility for access to classified information is denied.

_____
Robert J. Kilmartin
Administrative Judge