DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 12-08828
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Ray Blank, Esq., Department Counsel
For Applicant: *Pro se*

04/19/2017

_____

Decision

_____

KILMARTIN, Robert J., Administrative Judge:

Applicant did not mitigate the use of information technology systems and personal conduct security concerns. Eligibility for access to classified information is denied.

Statement of the Case

On November 2, 2015, the Department of Defense (DOD) issued a Statement of Reasons (SOR) to Applicant detailing security concerns under Guidelines M (use of Information technology systems) and E (personal conduct). The action was taken 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 (AG) implemented by the DOD on September 1, 2006.

Applicant responded to the SOR on November 16, 2015, and elected to have the case decided on the written record in lieu of a hearing. The Government's written case was submitted on March 25, 2016. A complete copy of the file of relevant material (FORM) was provided to Applicant, who was afforded an opportunity to file objections

and submit material to refute, extenuate, or mitigate the security concerns. Applicant received the FORM on April 25, 2016. In June 2016, Applicant responded with a two-page letter and 34 pages of documentation attached. These attachments have been collectively marked as Applicant Exhibit (AE) A and are admitted into evidence without objection.[1] The case was assigned to me on March 20, 2017. The Government exhibits identified as Items 1 through 9 included in the FORM are admitted in evidence.

Findings of Fact

Applicant is a 50-year-old employee of a defense contractor. He has worked in his current position, off and on, since 2006 for various contractors. He served honorably in the Air Force from 1986 - 1992. He has been married since 1986, and reports five adult children.[2] Applicant has been forward deployed to both Iraq and Afghanistan. Applicant reports previous security clearances going back to 1985, including a top secret clearance from 1989 - 2003, with no issues.[3]

Applicant was terminated by a federal contractor in 2003 for time card fraud.[4] Applicant was counseled for this same offense on previous occasions before he was terminated.[5] Yet, he listed the reason for leaving this employment as "end of contract" in section 13A of his 2012 SCA.[6] Applicant claims that he misunderstood the questions in the SCA to only require a seven-year look back.[7] Yet, in his subject interview in October 2008, Applicant contends that his termination actually resulted from a personality dispute with his supervisor at the time.[8] He suggests that his supervisor retaliated against Applicant who had earlier reported that supervisor for an unrelated security violation. Applicant has now admitted that he was terminated in 2003 for time-card fraud, but seems to deny that he actually committed that fraud.[9]

Applicant was terminated by another federal contractor-employer in 2011. In his 2012 SCA, Applicant claims that this was due to a reduction in force and restructure of

[1] AE A, attachments to Response to FORM, including 16 letters of recommendation; 4 certificates of appreciation; and 2 training certificates.

[2] GE 4 and 5.

[3] GE 7.

[4] GE 6, and GE 7 at page 1.

[5] GE 6.

[6] GE 5, at page 19.

[7] GE 2, Answer to SOR.

[8] GE 7.

[9] GE 2, Answer to SOR, and GE 7

the department.[10] Applicant later admitted that he was in fact fired due to misuse of his employer's laptop computer, by accepting pornographic images found there on his e-mail account. Applicant was aware of company policy regarding inappropriate materials on his computer but did not think that an IT scan of the computer would include this e-mail account.[11] Applicant claims that he did not list this reason for termination on his Questionnaire for National Security Positions/Security Clearance Application (SCA) because his employer told him not to discuss it, as it was confidential.[12] Applicant also claims that this matter was investigated previously by OPM and the outcome was favorable to Applicant.[13] However, he provided no documentation to corroborate these contentions.

Applicant is an Air Force Veteran and he raised five children. He provided 3 certificates of appreciation from his federal contractor-employer, a letter of appreciation from the U.S. Ambassador to Afghanistan, and 16 impressive letters of recommendation. These were attached to his Response to the FORM. All attest to his courage, professionalism, work ethic, honesty and integrity, especially while working overseas under adverse circumstances. He is obviously highly respected by his superiors, subordinates and peers and has contributed a great deal.

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 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."

[10] GE 5.

[11] GE 8 at page 2.

[12] GE 8, at page 2.

[13] GE 2, Answer to SOR.

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 M, Use of Information Technology Systems

The security concern for noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems, is set out in AG ¶ 39:

> Noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise a concern about an individual's reliability and trustworthiness, calling into question the willingness or ability to properly protect sensitive systems, networks, and information. Information technology systems include all related computer hardware, software, firmware and data used for the communication, transmission, processing, manipulation, storage, or protection of information.

The guideline notes several conditions that could raise security concerns under AG ¶ 40. The following is potentially applicable in this case:

> (e) unauthorized use of a government or other information technology system.

Applicant admits to using his employer's laptop to accept pornographic images on his personal e-mail account, in violation of that employer's policies. The evidence is sufficient to raise the above disqualifying condition.

Conditions that could mitigate the use of information technology security concerns are provided under AG ¶ 41. The following are potentially applicable:

> (a) 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 current reliability, trustworthiness, or good judgment;
>
> (b) the misuse was minor and done only in the interest of organizational efficiency and effectiveness, such as letting another person use one's password or computer when no other timely alternative was readily available; and
>
> (c) the conduct was unintentional or inadvertent and was followed by a prompt, good-faith effort to correct the situation and by notification of supervisor.

There is insufficient evidence in the written record for a determination that enough time has elapsed since the 2011 computer misuse, or that it happened under such unusual circumstances that it is unlikely to recur. Applicant failed to disclose this misuse on this April 2012 SCA. Although, he does not deny the presence of the pornographic images on his work computer, he seems to minimize the significance, or dispute the validity of his termination. It is not clear that he has fully accepted responsibility for this transgression. It continues to cast doubt on his current reliability, trustworthiness, and good judgment. AG ¶ 41(a) is partially applicable. None of the other mitigating conditions are applicable. I find that use of information technology systems concerns remain despite the presence of some mitigation.

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; 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 or other protected government 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, 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.

Applicant's time card fraud, and repeated counseling for that fraud, is substantiated by the Joint Personnel Adjudication System (JPAS) entries. He does not deny it in his Response to the FORM, but minimizes it by saying that he was fired for a one hour discrepancy. This repeated time card fraud betrays questionable judgment, an unwillingness to follow rules and regulations, and a significant misuse of his employer's time. AG ¶ 16(d)(4) applies.

Since Applicant denied any intent to provide false information on his SCA, his intent is an issue. Pursuant to ¶ E3.1.14 of DOD Directive 5220.6, the Government is responsible for presenting witnesses and evidence on facts alleged in the SOR that have been controverted. Intent can be inferred or determined from the circumstances. Applicant claims that he misread the question to only require a seven-year look back, with respect to his 2003 termination. Yet, Applicant has not yet accepted full responsibility for this fraud, despite repeated counseling, reflected in the JPAS entries. Instead, he blames it on a personality dispute with his supervisor, without providing a shred of evidence to document that dispute. This, combined with his failure to disclose the more recent 2011 computer misuse, leads me to believe that this was not an

oversight. Instead, Applicant deliberately failed to disclose the reasons for these two terminations on his 2012 SCA, rather than inadvertently omitting the true reasons. Therefore, the disqualifying condition at AG ¶ 16(a) applies. None of the conditions that could mitigate security concerns enumerated in AG ¶ 17 applies.

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 the facts and circumstances surrounding this case. I have incorporated my comments under Guidelines E and M in this whole-person analysis.

I also have evaluated this record in the context of the whole-person factors listed in AG ¶ 2(a). Applicant is an Air Force veteran and long-time defense contractor employee. He raised five children, and he has held a security clearance for most of his adult life. He is held in high regard by his friends and associates as evidenced by the 16 impressive character reference letters. Nonetheless, this information is not sufficient to overcome the recent security concerns raised by his misuse of his company computer, and his failure to disclose the reasons for his two terminations. It was incumbent on Applicant to produce information that sufficiently addresses the factual allegations in this case. He did not do so. Available information leaves me with doubts about his current suitability for access to classified information. Because protection of the national interest is the principal focus in these adjudications, any unresolved doubts must be resolved against the Applicant.

Overall, the record evidence leaves me with questions and doubts as to Applicant's eligibility and suitability for a security clearance. I conclude Applicant did not mitigate the personal conduct or use of information technology systems 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 M:	Against Applicant
Subparagraphs 1.a:	Against Applicant
Paragraph 2, Guideline E:	Against Applicant
Subparagraphs 2.a - 2.b:	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 Applicant eligibility for a security clearance. Eligibility for access to classified information is denied.

_____
Robert J. Kilmartin
Administrative Judge