DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 16-02178
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Charles C. Hale, Esq., Department Counsel
For Applicant: *Pro se*

01/16/2018

Decision

BENSON, Pamela C., Administrative Judge:

Applicant failed to mitigate the security concerns under Guideline M (Use of Information Technology) and Guideline E (Personal Conduct). Eligibility for access to classified information is denied.

Statement of the Case

On December 17, 2012, Applicant submitted a security clearance application (SCA). On September 10, 2016, 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). (Items 1 and 3) 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) effective within the DOD on September 1, 2006. On June 8, 2017, new AG were implemented and are effective for decisions issued on or after that date.[1]

Applicant answered the SOR on September 30, 2016, provided documents included in the record as Applicant's Exhibits (AE) A-F, and elected to have his case decided on the written record in lieu of a hearing. On October 31, 2016, Department Counsel submitted the Government's file of relevant material (FORM), including documents identified as Items 1 through 7. Applicant received the FORM on November 1, 2016. He was afforded an opportunity to file objections and submit material in refutation, extenuation, or mitigation within 30 days. Applicant responded to the FORM on December 5, 2016, providing documents to which Department Counsel had no objection. The document's in Applicant's FORM response are marked Applicant's Exhibits (AE) AA through FF, and admitted into evidence.[2] The SOR and answer (Items 1 and 2) are the pleadings in the case. Items 3 through 7 are admitted into evidence without any objection from Applicant. The Defense Office of Hearings and Appeals (DOHA) assigned the case to me on September 25, 2017.

Findings of Fact

Having thoroughly considered the evidence in the record, including Applicant's admissions, I make the following findings of fact: Applicant is 54 years old. He earned a bachelor's degree in 1986, and master's degrees in 1989 and 1997. He is married and has a son almost 18 years old. Applicant previously was employed by a federal government contractor from August 2005 to February 2012. He has been employed by another federal contractor since October 2012. (Item 3)

Applicant admitted, as alleged in SOR ¶¶ 1.a and 1.b, that he received a written reprimand from his former employer in about 2008 for alleged overuse of the internet, more as what would be considered incidental, and for violating their information technology (IT) policy for visiting inappropriate adult content links on Craigslist. He was interviewed by a corporate investigation unit for his IT system misuse. A few weeks later, Applicant reported with his manager to human resources (HR), where Applicant was given a written reprimand. (Item 2)

Applicant also admitted that, in a moment of boredom in late 2011, he again accessed the previously prohibited Craigslist adult content website on his work computer. He accessed possibly 30-40 objectionable Craigslist links over a couple of weeks during work hours. He stopped accessing these prohibited websites by early January 2012. Applicant was then contacted by the corporate investigations unit again. (Item 2)

[1] I considered the previous AG, effective September 1, 2006, as well as the new AG, effective June 8, 2017. My decision would be the same if the case was considered under the previous AG.

[2] Applicant marked his exhibits with double letters (AE AA – FF) in order to avoid confusion with the documents he marked as exhibits A – F in his response to the SOR.

In February 2012, HR told Applicant they were terminating him from employment. He was in the HR office processing paperwork, when during a break, he drafted a pre-dated resignation letter and gave it to an HR representative. Applicant submitted the predated resignation letter hoping his status would be labeled a "resignation" or a "resignation in lieu of termination" instead of a termination for cause. Applicant admitted SOR ¶ 1.c allegation, that he was terminated by his former employer in 2012 due to accessing prohibited websites on his government computer. (Item 2)

Applicant denied the SOR ¶ 2.a allegation that he intentionally falsified his December 2012 SCA, by answering "No" to the questions asking if within the last seven years of employment, had he received a written warning, been officially reprimanded, suspended, or disciplined for misconduct in the workplace, such as a violation of security policy. (Items 2 and 3) In response to the SOR, he claimed he had used a 2011 SCA to answer the same question cited in his 2012 SCA. (Items 2, 3 and 7) Applicant also stated he answered this question with a negative response because the question asked to disclose only violations of security policy in the workplace, and his misuse of his employer's IT system was not a violation of security policy.

Applicant's 2012 SCA's previous question also asked him if he had ever been fired by this employer, quit after being told he would be fired, left by mutual agreement following charges or allegations of misconduct, or left by mutual agreement following notice of unsatisfactory performance. Applicant also answered "No" to this question. Under "Optional Comment" Applicant disclosed he had resigned from this employment with separate plans to move. He also listed that he had resigned while there was an ongoing investigation for his internet access to Craigslist-only websites. Any later decision made by the employer on his exact exit status was not fully known by him. (Item 3) Applicant was told by his employer that he was being terminated for his repeated IT misconduct in February 2012. Applicant completed the SCA in December 2012. At least one of scenarios posed in the above question fit his situation. This information was not alleged under Guideline E, but I have considered it as probative of his state of mind when he completed the SCA.

Applicant provided numerous character reference letters as well as employee appraisals. Those documents show he is a valued, knowledgeable employee and that he has received positive peer and customer feedback. The reference letters did not indicate they were aware of the information in the SOR. Applicant has held different levels of security clearances over the 20 plus years he has been employed by federal government contractors.

Policies

When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the AG. In addition to brief introductory explanations for each guideline, the AG 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(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 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. 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.

Section 7 of EO 10865 provides that 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

The security concern relating to the use of information technology is set out in AG ¶ 39:

> 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.

AG ¶ 40 (e) (*unauthorized use of any information technology system*), applies to these facts and circumstances. Applicant admitted all three Guideline M allegations. He misused his former employer's IT system on more than one occasion, and repeated his misconduct after being specifically reprimanded for it.

The following mitigating conditions under AG ¶ 41 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 reliability, trustworthiness, or good judgment;
>
> (c) the conduct was unintentional or inadvertent and was followed by a prompt, good-faith effort to correct the situation and by notification to appropriate personnel; and
>
> (d) the misuse was due to improper or inadequate training or unclear instructions.

Applicant was reprimanded by his former employer in 2008 for misusing their IT system. He had been accessing the internet much more than what was permitted by his employer, and also for accessing inappropriate adult content on Craigslist. Following this reprimand, he was able to follow his employer's IT policy rules for a few years without mishap. In late 2011, while bored at work, Applicant returned to the misuse of his employer's IT system for a couple of weeks until early 2012. AG ¶ 41(a) does not apply because the misconduct did recur, and his repeated misconduct does cast doubt on his reliability, trustworthiness, and good judgment.

Applicant's conduct was not inadvertent. In addition, he never attempted any prompt or good-faith effort to notify appropriate IT corporate managers that he may have been accessing the internet more than what was considered incidental, or for accessing previously prohibited adult content on Craigslist in late 2011 to early 2012. AG ¶ 41(c) does not apply.

Applicant received a reprimand on a written document expressly prohibiting his overuse of the internet, generally, and specifically prohibiting his assess to any website

that contained inappropriate adult content. He accessed inappropriate adult content in the Craigslist Personals section in 2008. He repeated that conduct again in 2011 to early 2012, despite the previous reprimand by his employer. AG ¶ 41(d) does not apply.

Guideline E: Personal Conduct

AG ¶ 15 expresses the security concern for personal conduct:

> 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(a) applies to these facts and circumstances: 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 national security eligibility or trustworthiness, or award fiduciary responsibilities.

Applicant did not disclose on his 2012 SCA when asked whether within the last seven years, had he received a written warning, been officially reprimanded, suspended, or disciplined for misconduct in the workplace, *such as for a violation of security policy*, (emphasis added). The phrase "such as" shows that a violation of security policy is merely an example of misconduct in the workplace. Applicant answered this question with a negative response. He stated that this question only pertained to violations of security policy in the workplace, and he denied that his IT system misconduct was a violation of security policy. He also stated that he used his response from his 2011 SCA to answer this question. It is clear when reading the question in his 2011 SCA that the phrasing *does limit* (emphasis added) disclosure to violations of security policy only, and that is because the previous question in the 2011 SCA required disclosure of any type of misconduct in the workplace. In the 2012 SCA, however, the authors of the revised SCA combined the two questions into one question. It is clear from the revised question that any misconduct, to include violations of security policy, were required to be disclosed. There is sufficient evidence to show his omission was intentional to support the application of the above disqualifying condition.

The guideline also includes conditions that could mitigate security concerns arising from personal conduct. The following mitigating conditions under AG ¶ 17 are potentially applicable:

> (a) the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts; and

> (b) the offense is so minor or so much time has passed, or the behavior is so infrequent, or 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.

Applicant did not make prompt, good-faith efforts to correct the omission on his December 2012 SCA. His failure to be completely honest about the circumstances of his reprimands casts doubt on his reliability, trustworthiness and good judgment. There is insufficient evidence to support the application of the above mitigating conditions.

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 Guideline M and Guideline E in my whole-person analysis. Applicant has performed productively for more than 20 years. He provided several character reference letters and employee appraisals with his documentation; however, the persuasive value of that information is lessened because there is no indication the authors were aware of the adverse conduct at issue here. In the face of his repeated acts of misuse of his employer's IT system, and his failure to be completely candid on the 2012 SCA, his favorable character evidence alone is not enough to absorb security concerns in this case.

Applicant repeated misuse of IT systems after being reprimanded for this same type of behavior shows that he is not trustworthy. He is a mature adult with three college degrees, and knew, or should have known, his conduct was unacceptable. Likewise, his 2012 SCA falsification was deliberate and his explanations for the omission were not credible. Overall, the record evidence leaves me with doubts as to Applicant's good judgment, reliability as well as eligibility and suitability for a security clearance. Because

protection of the national interest is the principle focus of these adjudications, any unresolved doubts must be resolved against the granting of access to classified information.

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-1.c:	Against Applicant
Paragraph 1, Guideline E:	AGAINST APPLICANT
Subparagraphs 2.a:	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 security to grant Applicant's eligibility for a security clearance. Eligibility for access to classified information is denied.

Pamela C. Benson
Administrative Judge