DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
----------	)	ISCR Case No. 14-02823
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Alison O'Connell, Esquire
For Applicant: Eric A. Eisen, Esquire

04/30/2015

_____

Decision

_____

MARSHALL, Jr., Arthur E., Administrative Judge:

Applicant failed to mitigate the Government's security concerns under Guideline E and Guideline M. Applicant's eligibility for a security clearance is denied.

Statement of the Case

On August 25, 2014, the Department of Defense (DOD) issued Applicant a Statement of Reasons (SOR) detailing security concerns under Guideline E (Personal Conduct) and Guideline M (Misuse of Information Technology Systems). The action was taken under Executive Order 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 within the DOD on September 1, 2006.

In a letter dated September 16, 2014, Applicant admitted in part, and denied in part, the Guideline E allegations at ¶¶ 1.a and 1.b, and denied the allegation at ¶ 1.c. In addition, he admitted the sole allegation under Guideline M, ¶ 2.a. Applicant then requested a hearing before an administrative judge from the Defense Office of Hearings and Appeals (DOHA). I was assigned the case on January 29, 2015. DOHA issued a

notice of hearing on March 2, 2015, setting the hearing for March 12, 2015. The hearing was convened as scheduled.

The Government offered three documents, which were accepted without objection as exhibits (Exs.) 1-3. Applicant offered testimony and five files of documents, which were accepted into the record without objection as exhibits Exs. A-E. On March 20, 2015, the transcript of the proceeding (Tr.) was received. The record was then closed.

Findings of Fact

Applicant is a 58-year-old division director working in the area of cybersecurity. He has been with his present employer for about four years. Applicant has earned a bachelor's degree in science and two master's degrees, one in business and one in security. He served as an officer in the United States military for 30 years, retiring in 2009. Applicant is married and has four children. Applicant submitted excellent recommendations from senior government officials concerning his integrity and reliability; from professional peers regarding different stages of his career; from superiors regarding Applicant's work performance; and both citations and commendations from the highest levels regarding his military service. (Tr. 14-16; Exs. A-E) He has had an impressive military career.

At his retirement ceremony in 2009, Applicant was approached by an individual working for a Defense contractor. He was invited to visit the company, which he did. After the visit, he accepted a job offer from the business as a military account executive. Applicant thought that meant he would be helping the U.S. military and the company define requirements, then turn them into missions. (Tr. 35) He believed this position, which paid $250,000 a year, was a way for the company to tap into his strengths at "marshaling resources to achieve ends." (Tr. 35-36; 65) The job required him to sign in and out for when he worked. The general company ledgers paid Applicant's salary; he did not have billable hours for specific clients. (Tr. 77)

In fact, the company wanted Applicant for his professional contacts, his ability to introduce company officials to his former contacts and friends, and to share certain non-public data projections he had worked on before his retirement. (Tr. 36) Applicant was not permitted to divulge such data. As the true nature of his job became clearer to him, Applicant found the company's targeted "door opening" aspects to be "humiliating," and a betrayal to his former friends and colleagues. (Tr. 37-38) He also realized he was not very good in the job as contemplated. (Tr. 37) Within a few months, the company stopped using Applicant, making him feel isolated. (Tr. 39) For something to do, he started surfing the Internet. (Tr. 40) At first he would look at various social media sites, mostly to "kill time." (Tr. 41)

In approximately August 2010, one such social media site led Applicant to a pornography site. (Tr. 66) Applicant knew it was against company policy for him to view pornography on his work computer. (Tr. 65) When he tried to cancel the window, more

windows and images cascaded across his computer screen. It appeared the company had no unfiltered access to the Internet. As the images appeared, he "lingered too long on those sites." (Tr. 44) Over a week, he spent "10 minutes, 15, 20, or thereabouts" purposely looking at pornography. (Tr. 44; *see also* Tr. 66-67) Sometimes he accessed pornography deliberately and directly, rather than through his social media portal. (Tr. 67-68; 100) Applicant did not report the pornography, pop-ups, or cascades. (Tr. 45)

Several days later, the technology team removed Applicant's computer for examination. Soon thereafter, his supervisor, another former military officer, invited Applicant to a conference room in a different building. There, the men were met by another individual who sat nearby, silently. The supervisor began speaking about the pornography found on Applicant's computer. (Tr. 47) At that point, Applicant said he understood that the "company didn't want [him] anymore . . . that they were asking [him] for things [he] could not deliver." (Tr. 48) His supervisor countered with "this is going to adversely affect you," to which Applicant commented "'no need to go any further. That's fine.'" (Tr. 48) The supervisor then stated, "[L]ook, just resign. You resign and this is over. You part ways with the company." (Tr. 48) No issue was raised as to whether Applicant had billed customers for the time he spent looking at pornography. The men shook hands, and Applicant obtained permission to retrieve his possessions from his office that weekend. Applicant then signed a piece of paper the supervisor asked him to sign, but Applicant is unsure whether it was a resignation letter. (Tr. 74-75) He believed that this put an end to all issues – the "whole situation" - both in terms of pornography and their mutual displeasure with Applicant's placement at the company, and that no repercussions would result from his actions. (Tr. 88; 96)

About a year later, in 2011, Applicant was recruited for a cybersecurity position with another company. In November 2011, Applicant was interviewed by an authorized DOD investigator. During the interview, Applicant initially stated that he did not have any problems at his last position. He stated that he left that job to pursue a better opportunity elsewhere.

In completing a security clearance application (SCA) in May 2013, Applicant answered "no" to the question: "For this employment have any of the following happened to you in the last seven (7) years? Fired; Quit after being told you would be fired; Left by mutual agreement following charges or allegations of misconduct; Left by mutual agreement following notice of unsatisfactory performance." He answered in this way because it was his interpretation of the meeting with his former supervisor that an executive decision had been made that if he walked away from his job, it would put an end to any discussion about the pornography on his computer.[1] (Tr. 54, 87) In addition, he thought it was the company's way of getting rid of him since he could not provide it

[1] When asked, "is what happened in fact that you left by mutual agreement after discussion had been made about something that shouldn't have happened?" Applicant answered "That's correct. . . . I should have put it that way. And as I've said, I believe that if I had to go back today and do it that's exactly what I should've put that day, but I did not." (Tr. 87-88) When asked if it was his assumption that "by leaving as you did that the whole thing would be [swept under] the rug, there would be no further repercussions from it," Applicant stated, "Sir, that was my understanding." (Tr. 88)

with the data it sought from him. (Tr. 55) In response to the SCA question as to why he left his employment, Applicant wrote that he left to start a business of his own. (Tr. 83; Ex. 1 at 12-13 of 41) Applicant's belief that the slate must have been made clean regarding the pornography issue was fortified in 2011 because he still had a security clearance. (Tr. 85, 88)

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 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 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. Likewise, I have not drawn 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 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.

Section 7 of Executive Order 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 Systems

Under AG ¶ 39, noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual's reliably 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.

AG ¶ 40 describes conditions that could raise a security concern and may be disqualifying. Here, Applicant knew his employer prohibited the use of its computers to view pornography. Moreover, Applicant admitted that he viewed such material on his office computer. Consequently, after reviewing the disqualifying conditions under AG ¶ 40, I find AG ¶ 40(e) (unauthorized use of a government or other information technology system) applies.

I also considered all of the mitigating conditions under AG ¶ 41. Applicant, after maintaining a security clearance for several years, knowingly viewed pornography and searched for pornographic content on a workplace computer in 2010. He knew viewing such material at work was prohibited. He failed to timely report to appropriate personnel his initial, unintentional exposure to such material. He then failed to report his intentional pursuit of such material later that week. The following year, he failed to disclose that his viewing of pornography jeopardized his terms of employment during a 2011 job interview. He similarly failed to disclose that fact on his SCA, preferring instead to suggest a different reason for his departure. Applicant remains less than straightforward in detailing the events at issue, and his interpretation of the exchange between himself and his supervisor in 2010 stretches credulity. Such considerations obviate applicability of AG ¶ 41(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*).

Finally, Applicant is well-versed in the area of cybersecurity. He knows the risks associated with pornography sites from a security standpoint, and knows that viewing pornography in the workplace is generally barred. In his particular workplace, pornography had no part in their organizational mission. Moreover, Applicant's viewing of pornography went from inadvertent to intentional, yet he never advised the proper authorities of his accessing of such material on his work computer. Such facts obviate applicability of AG ¶ 41(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*).

Guideline E, Personal Conduct

The security concern for personal conduct is set out in AG ¶ 15, where the significance of conduct involving questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations is defined (*[p]ersonal conduct 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.

In 2010, despite a company policy to the contrary, Applicant surfed for pornography on his work computer. Its discovery led to his being given the opportunity to resign, rather than face potential workplace personnel repercussions. In 2013, he completed a SCA. On that form, he forewent admitting that he left his position by mutual agreement following charges or allegations of misconduct, and wrote that he left to start his own business. He did so under the impression that the agreement would make the pornography issue unverifiable. Such facts are sufficient to raise Personal Conduct Disqualifying Conditions AG ¶ 16(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*); AG ¶(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 AG ¶16(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* . . .).

Applicant intentionally falsified facts on his SCA and misled DOD investigators regarding his 2010 separation from employment. The facts all suggest that, thinking the proffered agreement with his former supervisor meant the facts regarding his pornography viewing would not leave the company, Appellant assumed the issue was settled and put to rest. Consequently, the reason for his departure would never be divulged or used for purposes of verification. What personnel may do with information about an employee and how the Government might proceed on information raising security concerns regarding one maintaining a security clearance, however, are distinctly separate processes. They reflect different interests. To falsify or mislead based on the impression one will not get caught constitutes risky behavior and poor judgment.

The following personal conduct mitigating conditions potentially apply:

AG ¶ 17(a) (the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts);

AG ¶ 17(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);

AG ¶ 17(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

AG ¶ 17(e) (the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress).

Applicant intentionally concealed, then delayed revealing, the facts and circumstances surrounding his final meeting with his supervisor in 2010. Now nearly four years later, he acknowledges the truth. At best, AG ¶ 17(e) applies to a limited extent. .

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). 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 incorporated my comments under the guidelines at issue 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 58-year-old man working for a defense contractor. His military career was stellar, and he has been highly commended and awarded in his fields of expertise. He has a bachelor's degree and two master's degrees. He has considerable expertise with computers and in cybersecurity. In 2009, while working in the private sector after his retirement from the military, he encountered pornography on his work computer. At first it was accidental, then he began to search for it himself. His employer had a policy against such viewing. A week later, he was called into a meeting to discuss the fact pornography had been found on his work computer. The discovery came at the

apex of his frustration with the company, and accepting its offer to resign seemed like a welcome opportunity to get a fresh start without making more of his surfing for pornography. While personnel actions were curtailed, the related security concerns that had been raised worked their way through their own process. Eventually, that process caught up with Applicant.

Applicant took a risk when he concealed the truth when meeting with DOD investigators and in completing his 2013 SCA. That risk failed to pay off when the security clearance process persisted on the report that Applicant had viewed pornography in 2010. While Applicant argues that the agreement to resign was executed for multiple reasons, the meeting was initiated to discuss pornography. It was to that meeting his supervisor brought a witness and a prepared resignation form. While Applicant was given a graceful way of terminating his tenure, the facts presented give no realistic basis for one to assume the pornography issue was dead on all fronts. In light of the foregoing, I find that Applicant failed to mitigate 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
Subparagraphs 1.a-1.c:	Against Applicant
Paragraph 2, Guideline E:	AGAINST APPLICANT
Subparagraph 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 interest to grant Applicant a security clearance. Eligibility for access to classified information is denied.

_____
Arthur E. Marshall, Jr.
Administrative Judge