DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 18-02150
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Alison O'Connell, Esq., Department Counsel
For Applicant: Bradley P. Moss, Esq.

03/12/2020

_____

Decision

_____

LOUGHRAN, Edward W., Administrative Judge:

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

Statement of the Case

On August 23, 2019, the Department of Defense (DOD) issued a Statement of Reasons (SOR) to Applicant detailing security concerns under Guidelines E (personal conduct) and M (use of information technology). Applicant responded to the SOR on September 12, 2019, and requested a hearing before an administrative judge. The case was assigned to me on November 26, 2019. A hearing scheduled for January 29, 2020, was cancelled. The hearing was convened as rescheduled on February 20, 2020.

Evidence

Government Exhibits (GE) 1, 2, 3, 5, and 6 were admitted in evidence without objection. The objection to a section of GE 4 was overruled, and GE 4 was admitted in its entirety. Applicant testified and called two witnesses. Department Counsel objected to the testimony of one of Applicant's witnesses on the grounds that the witness was not

an expert and the testimony was not relevant. The objections were overruled. Applicant's Exhibits (AE) 1 through 11 were admitted without objection. The record was held open for Applicant to submit additional information. He submitted documents that I have marked AE 12 through 15 and admitted without objection.

Findings of Fact

Applicant is a 45-year-old employee of a defense contractor. He served in the Air National Guard from 1996 until he was honorably discharged in 2002. He graduated from law school in 2008. He is married with children. (Transcript (Tr.) at 57, 159; GE 1-3; AE 9)

Applicant worked in software development before he went to law school. He practiced law for a period, but then went back to software development. He worked for a defense contractor from 2009 to 2017, primarily as a software developer and system administrator at a DOD agency. (Tr. at 57-60, 87; GE 1-3)

In August 2017, the DOD agency notified the Inspector General (IG) that during routine monitoring of Internet usage and network traffic, they detected that Applicant used a government information technology (IT) system to view illicit material containing sexual content, which was against the agency's IT policy. The report indicated:

- In January 2017, Applicant searched Google for "girl rubbing herself." The search contained nude images and sexual content.

- In June 2017, Applicant searched Google for "rubbing her [vulgar term for vagina]." The search contained nude images and sexual content.

- In June 2017, Applicant searched Google for "female oral." Applicant then viewed several pages of nude images of men and women engaged in sexual acts. (GE 4)

The agency further reported that since 2012, Applicant had been involved in 19 other cases of unauthorized software downloads. The software included graphics, audio and music editing software, bar examination preparation software, and text editing software. The agency noted that Applicant was sent a user account-violation warning letter on a specific date in April 2016. (GE 4, 5)

In August 2017, Applicant's access to the DOD agency's network was suspended, and he was escorted off the premises. He asserted that he was not told the reason. He wrote an e-mail with a copy to the IG. He thought the IG might already have an open investigation, and he was "concerned that [he] was being inappropriately removed" from the contract. He wrote: "If the reason that I'm being removed for is working on [an]other project for another company, during contract hours, I would like to explain." He indicated that during lulls in work or when he needed a break, he would practice programming on his personal websites. (Tr. at 111-117; GE 4, 6)

The IG obtained a report of Applicant's unclassified Internet usage. From March 2017 through August 2017, Applicant visited his personal websites 1,015 times. The IG contacted an unidentified individual, who stated that Applicant's use of his personal websites for duty-related purposes was not in compliance with the contract statement of work (SOW). (GE 6)

Applicant was interviewed over the telephone by an IG investigator in December 2017. He stated that he used his personal websites to practice programming and develop solutions for site problems at the DOD agency. He estimated that from March 2017 to August 2017, he visited his personal websites about three to four times per week, for up to two hours per day. The IG estimated that equated to between 150 and 200 hours at an hourly rate of $153, or between $23,071 and $30,762. The IG concluded that Applicant committed contractor cost mischarging (labor hours) when he submitted fraudulent timesheets that included 150 to 200 hours that he spent working on tasks not specified in the contract SOW. The U.S. Government apparently recouped an amount in the above range from a defense contractor. (Tr. at 113-121, 148-151; GE 6)

Applicant denied some of the conduct and explained the rest. He admitted that he downloaded software, but he stated that it was primarily for his job. He was a data transfer officer (DTO) who would download items for others. He admitted downloading a few programs that were not for his job, such as a Sudoku solver and an audio manipulation program that he used to make old songs sound better. He does not recall downloading the bar examination preparation software, but he surmises that he likely did. He stated that employees were permitted incidental non-official use of their computers, and he did not realize that he was unauthorized to download any of the software. He denied ever receiving a warning letter. He stated that the only thing he was told was that the Sudoku solver was unauthorized, and it was deleted from his system. (Tr. at 59-70, 85-86, 123-127, 153-155; Applicant's response to SOR)

Applicant denied intentionally submitting fraudulent timesheets. He asserted that his use of his websites was to hone his skills as a software developer or to benefit the DOD agency. Additionally, incidental non-official use of the computer was permitted. (Tr. at 59-60, 86-101, 141-153, 156-159; AE 5-7)

Applicant admitted that he conducted the Google searches on the government IT system, which revealed inappropriate material, but he denied that he viewed sexually explicit material. Applicant was involved in an online affair with a woman he had never met in person. The affair included graphic chats and exchanges from his phone, which involved sexually explicit materials and "phone sex." He wanted to send her flirtatious and suggestive material with "non-explicit but sexual images" using the GIF (Graphics Interchange Format - short animated or moving pictures) format over the government IT system. He knew the system had SafeSearch, which would screen out most, but not all, graphic materials. He admitted that even with SafeSearch on, he "came across explicit images a few times. [He] did not download these and browsed away quickly, or closed the browser." He also admitted that he "had several inappropriate text conversations"

with the woman from a government computer. (Tr. at 71-77, 82-84, 102-106, 128-141, 155-156; Applicant's response to SOR; GE 2, 3; AE 3, 4, 15)

Applicant described one of the GIFs he sent as what appeared to be a man performing oral sex on a woman. Another was of a woman with her hand inside her underwear apparently masturbating. He asserted that there was no visible nudity or genitalia in any of the GIFs. (Tr. at 71-72, 83-84, 133-134; GE 2, 3; AE 3)

Applicant stated that his affair with the woman ended in August 2017, a few days before he was removed from the contract. He asserted that he was never told why he was removed from the contract. He thought the affair itself, but not necessarily the inappropriate searches, might have been discovered. He stated that he did not think the inappropriate searches and images were an issue until he thought it through about a week or two after he was removed from the contract. He told his wife of the online affair in August 2017. He also sought advice and counseling through his church. (Tr. at 78-80, 101, 106-113; AE 4, 9, 14)

Applicant thought the affair could have been "a point of blackmail." He indicated that he "drafted a letter to self-report in August of 2017 but was advised to not report by a trusted advisor." He discussed the information during his background interview in March 2018. He reported the information to his facility security officer (FSO) in April 2018. In that report, he indicated the incidents happened "[d]uring a rough patch in [his] marriage in May-July 2017." When asked at hearing how that accounted for his search in January 2017, he stated that he and the woman were friends before January 2017, and the flirtatious behavior, but not the full online affair, started in January 2017. (Tr. at 78, 107-111, 131-132; AE 4, 14)

Applicant apologized for his inappropriate conduct. His actions cost him his job and almost his marriage. He asserted that he has learned a valuable and costly lesson, and that the conduct will not be repeated. (Tr. at 81-82, 121-122, 137)

Applicant volunteers in his community, and he is active in his church. He submitted documents and letters attesting to his moral character and excellent job performance. He is praised for his work ethic, honesty, trustworthiness, judgment, loyalty, strength, determination, dependability, integrity, and willingness and ability to protect classified information. He is recommended for a security clearance. (Tr. at 18-35, 51-54; AE 8-13)

Policies

This case is adjudicated 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), which became effective on June 8, 2017.

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 national security eligibility will be resolved in favor of the national security."

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

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

> (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.

Applicant used a DOD agency's IT system to view illicit material containing sexual content, which was against the agency's IT policy. He also downloaded software onto the agency's IT system without authorization. The above disqualifying conditions are applicable.

Conditions that could mitigate the use of information technology systems 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 reliability, trustworthiness, or good judgment; and
>
> (b) the misuse was minor and done solely in the interest of organizational efficiency and effectiveness.

Applicant downloaded software onto the agency's IT system without authorization. I do not find that conduct, as alleged in SOR ¶ 1.a, warrants the loss of Applicant's security clearance, and it is mitigated.

I am convinced that Applicant received a user account-violation warning letter in April 2016. Applicant is an attorney, a software developer, and a system administrator. He did not need that letter to know that his Google searches on the government IT system for sexual materials were forbidden. However, the letter served to firmly place him on notice that further misconduct would not be tolerated. Applicant admitted that his searches revealed sexually explicit images on two occasions, which means he went back at least once after he knew that sexually explicit materials could result. Additionally, I am not convinced that Applicant has been completely candid. His conduct continues to cast doubt on his reliability, trustworthiness, and good judgment. AG ¶¶ 41(a) and 41(b) are not applicable to the conduct alleged in SOR ¶ 1.b.

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:

> (c) credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any other single guideline, but which, when considered as a whole, 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 individual may not properly safeguard classified or sensitive information;
>
> (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 individual may not properly safeguard classified or sensitive information. This includes, but is not limited to, consideration of:
>
> > (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 by a foreign intelligence entity or other individual or group. Such conduct includes:
>
> > (1) engaging in activities which, if known, could affect the person's personal, professional, or community standing.

The use of information technology security concerns are cross-alleged under Guideline E. That conduct reflects questionable judgment and an unwillingness to comply with rules and regulations. It also created vulnerability to exploitation, manipulation, and duress. AG ¶ 16(e) is applicable. AG ¶ 16(c) is applicable to the allegation that Applicant downloaded software onto the agency's IT system without authorization. It is not perfectly applicable to the allegation that he used a DOD agency's IT system to view illicit material containing sexual content because that conduct is sufficient for an adverse determination under the use of information technology guideline. However, the general concerns about questionable judgment and an unwillingness to comply with rules and regulations contained in AG ¶¶ 15 and 16(c) are established.

Also alleged under Guideline E is that Applicant submitted fraudulent timesheets and overcharged the Government for approximately 150 to 200 hours of work, which amounted to about $23,000 to $30,000. I am satisfied that Applicant used his computer for non-official purposes. Like virtually every employee, there were times when he was on the clock but not actually working. I am not convinced that it rose to the level of "a pattern of dishonesty or rule violations," or "significant misuse of Government or other employer's time or resources." SOR ¶ 2.b is concluded for Applicant.

AG ¶ 17 provides conditions that could mitigate security concerns. The following are potentially applicable:

> (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.

The above analysis under the use of information technology guideline applies here. The allegation that Applicant downloaded software onto the agency's IT system

without authorization is mitigated. The allegation that he used the agency's IT system to view illicit material containing sexual content is not mitigated. That conduct continues to cast doubt on his reliability, trustworthiness, and good judgment. The above mitigating factors, individually or collectively, are insufficient to dispel the personal conduct security concerns.

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(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 have incorporated my comments under Guidelines E and M in my whole-person analysis. I also considered Applicant's strong character evidence, but the favorable information is insufficient to overcome his incidents involving questionable judgment and an unwillingness to comply with rules and regulations.

Overall, the record evidence leaves me with questions and doubts about Applicant's eligibility and suitability for a security clearance. I conclude Applicant did not mitigate the personal conduct and use of information technology 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
Subparagraph 1.a:	For Applicant
Subparagraph 1.b:	Against Applicant

Paragraph 2, Guideline E:	Against Applicant
Subparagraph 2.a:	Against Applicant
Subparagraph 2.b:	For Applicant

Conclusion

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.

_____
Edward W. Loughran
Administrative Judge