DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	
----------	)	ISCR Case No. 17-03361
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Nicole A. Smith, Esq., Department Counsel
For Applicant: Leon J. Schachter, Esq.

12/06/2018

Decision

KATAUSKAS, Philip J., Administrative Judge:

Applicant contests the Defense Department's intent to deny his eligibility for access to classified information. He presented sufficient evidence to explain, extenuate, or mitigate the security concern stemming from his use of information technology. Accordingly, this case is decided for Applicant.

Statement of the Case

On October 17, 2017, the Department of Defense (DOD) Consolidated Adjudications Facility (CAF) sent Applicant a Statement of Reasons (SOR) alleging that his circumstances raised a security concern under Guideline M for his use of his employer's information technology.[1] Applicant answered the SOR on November 17, 2017, and requested a hearing.

[1] This action was taken under Executive Order (E.O.) 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended, as well as Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive). In addition, the *Adjudicative Guidelines for Determining Eligibility for Access to Classified Information* (AG), effective within the Defense Department on June 8, 2017, apply here.

On August 15, 2018, a date mutually agreed to by the parties, a hearing was held. Applicant and one character witness testified, and the exhibits offered by the Government and by Applicant were admitted into the administrative record without objection. (Government Exhibits (GE) 1 and 2; Applicant Exhibits (AE) F through L.)[2] The transcript of the hearing (Tr.) was received on August 21, 2018.

Procedural Issues

At the outset of the hearing, counsel for Applicant moved to dismiss the SOR on the grounds that the SOR, the Answer, GE 1, and GE 2 failed to state a *prima facie* case for disqualification under Guideline M. The Government objected on a number of grounds, principally that administrative judges do not have the authority under the Directive to grant motions to dismiss and that Applicant's admissions in the Answer and GE 2 made out a *prima facie* case. Applicant's counsel countered that the Directive is silent on whether administrative judges have the authority to grant such motions, but it does expressly grant the authority to rule on matters of procedure.[3] The Directive does expressly grant judges the authority to "rule on questions on procedure, discovery, and evidence . . . ."[4] I denied the motion on the grounds that a motion to dismiss is not a question of procedure but rather goes to the merits of the case.[5]

Findings of Fact

Applicant is 58 years old, married, and has two adult children, a son and a daughter. He has a Bachelor of Science in Electrical Engineering and Mathematics, a Master of Science in Electrical and Computer Engineering, and a Doctorate in Engineering Sciences. Applicant is a nationally known expert in electronic security. He has worked for his current employer, a defense contractor, since February 1991.[6]

The SOR made two allegations under Guideline M. First, it alleged that Applicant used his company laptop to view pornography from about December 2015 to December 2016. Second, it alleged that Applicant violated his employer's policy when he used his home network, instead of his employer's virtual private network (VPN) to establish a network connection on his company network, from about December 2015 to December 2016.[7] Applicant admitted that he viewed pornography on his company laptop but did so

[2] Applicant attached to his Answer documents that he marked as AE A through AE E.

[3] Tr. 9-15.

[4] Directive ¶ E3.1.10.

[5] Tr. 16.

[6] Tr. 20-23; AE A; AE F.

[7] SOR ¶ 1. "A virtual private network (VPN) extends a private network across a public network, and enables users to send and receive data across shared public networks is if their computing devices were directly connected to the private network. Applications running across a VPN may therefore benefit from

at home, during non-workhours and that at the time he did not believe his company's policy prohibited such use. Applicant denied that establishing a network connection using his home network instead of using his employer's VPN violated company policy.[8] As a result of those alleged security violations, Applicant was given a warning, a two day suspension (unpaid leave), and his access to classified information was taken away.[9]

In his Answer, Applicant cited a number of extenuating circumstances he faced during the time he was viewing pornography, which he claimed caused him to suffer from "a temporary lapse of judgment." First, there was "great personal loss" caused by the deaths of two very close family members. Second, Applicant and his wife were experiencing a "particularly challenging time in their marriage." Third, he was managing his career and his diabetes diagnosis. Applicant very much regrets his behavior. He and his wife are seeing a marriage counselor, and Applicant is also seeing a counselor on his own.[10]

Applicant submitted his company performance evaluations for 2014 through 2017. He is regularly praised for his technical expertise, his broad knowledge, and his interpersonal and communication skills. Applicant displays an "engaging ability to explain complex topics in understandable terms."[11]

Applicant submitted three character affidavits of professional colleagues who have known him for 10 to 20 years. Each affiant had reviewed the SOR. Nonetheless, they uniformly praised his reliability, integrity, and trustworthiness and that Applicant is worthy of holding a security clearance.[12]

Applicant's spouse of more than 30 years also submitted an affidavit. While she knows that Applicant has viewed pornography and finds it offensive, it is not a significant factor in their marriage difficulties. She also observed that the recent deaths of two close family members caused Applicant stress and deep grief. She said that Applicant's sense

---

the functionality, security, and management of the private network." https:en.wikipedia.org/wiki/Virtual_private_network, *citing* Mason, Andrew G., *Cisco Secure Virtual Private Network* at 7 (Cisco Press 2002).

[8] Answer ¶¶ 1.a-1.b. Applicant viewed pornography about three to four times per week. GE 2, p. 1.

[9] GE 2, pp. 5-6. Applicant was allowed to serve the suspension during the Christmas holidays. *Id.,* p. 3.

[10] Answer ¶ 1.a. Applicant's wife knows about his viewing of pornography but has no interest in participating. GE 2, pp. 1-2; AE C5. Applicant also told his children and certain co-workers about security issues. GE 2, p. 6.

[11] AE B1-B3; AE I.

[12] AE C1-C3. Applicant's character witness testified and simply adopted his character affidavit, AE C3. Tr. 43-46. AE C4 was identified on the exhibit list as being attached to the Answer, but it was not in the Answer that I was provided.

of duty, patriotism, and personal honor would never let him improperly divulge classified information.[13]

After losing his access to classified information, Applicant began seeing a clinical therapist in about February 2017.[14] Applicant submitted a July 26, 2018 letter from his licensed clinical therapist, whom he had been seeing weekly since March 16, 2017. The therapist reported that Applicant sought her help so that his viewing of pornography would not recur. She stated that he is "committed to the therapeutic process" so that he would not revert to viewing pornography. In her opinion, Applicant does not have any mental health disorder or personality traits that warrant any concern for his ability to function in a work environment.[15]

Applicant submitted a March 15, 2018 report of an evaluation conducted on February 2, 2018, by a licensed psychologist who was retained by Applicant's counsel. The psychologist reviewed the SOR, interviewed Applicant for about three hours, and administered a well-known psychological test. Applicant produced valid test results, from which the psychologist concluded that Applicant is "honest, regardless of incentives and temptations to be dishonest." The psychologist also found that Applicant does not warrant any mental health diagnosis and that he "does not suffer from an addiction to pornography, and his inappropriate use of pornography is something he has already discontinued without problem." The final psychologist's conclusion was that Applicant is "fit to hold any security clearance that is relevant for his job duties and that he will not deviate from expected procedures in the future."[16]

Applicant testified about his viewing of pornography on a company laptop. He was authorized to take his company laptop home, when he was on business travel, and to use it after work hours. He rationalized viewing pornography on his company laptop, because he was at home, after work, was not connected to his office network, and was not sending out any confidential information. In addition, Applicant's home network is password protected. It was as if he had simply inserted a DVD containing pornography on his company laptop after work hours. Applicant presumes, but does not know, that his company monitored its laptop's logs to keep track of network transactions, and that his transactions viewing pornography were in those logs. It was only after that discovery that he was made aware that viewing pornography was contrary to company policy. Applicant will never again view pornography on his company laptop. At the time, however, he did not believe that viewing pornography outside of work hours, at home, on a company laptop not connected to the company network, was a security violation.[17]

[13] AE C5.

[14] GE 2, p. 4.

[15] AE G2.

[16] AE G1.

[17] Tr. 25-27, 33-34. This is consistent with Applicant's May 16, 2017 Affidavit. GE 2.

Applicant testified about his use of his home network instead of his company's VPN to establish a network connection on his company laptop. He believed that the use of the company VPN was optional, not mandatory. In fact, his company's IT department and its cybersecurity staff recommended that he not use the company's VPN so he could access certain sites that were blocked on the corporate network. Using his own network instead of his company's network was not an attempt to evade discovery of his viewing of pornography. Applicant knew at all times that his use of the company laptop would be monitored by the company. If he wanted to evade discovery, he could have deleted or edited the logs on his company laptop or used anonymous sources. He did neither.[18]

Applicant explained several reasons for not using the company's VPN. First, although the VPN works fine when in the home office, during business travel it is unreliable. He travels extensively and not being able to work on his company laptop two weeks out of a month because the VPN is not functioning is a hindrance. Second, certain applications do not work on the VPN. For example, one application (web conferencing) works while at the home office, but outside of the home office it does not work on the VPN. Third, when the VPN breaks down, there is a risk to the entire system. Once when that happened, it wiped out his computer, and they had to reinstall the entire operating system. On another occasion, there were some incorrect settings, and for two weeks the VPN did not work.[19]

The following are the pertinent provisions of the company's VPN Policy (called "Wireless Networking and Mobile Device Practice"):[20]

• The policy covers "Wireless devices" (which includes laptop computers) (section 1.2).

• The policy covers "Wireless networks" (section 1.2).

• The policy applies to both company-owned and personally-owned equipment (section 1.3).

• When the employee is away from the home office, the policy states: "You may use all forms of wireless communications devices. To reduce risk, we *recommend* that you: • *Connect to known, password-protected networks where possible;*

• If using a [company computer], immediately establish a VPN connection to the [company] network. This will encrypt all data traffic and will provide [company] network protections" (section 2.2). (Emphasis added.)

[18] Tr. 27-29.

[19] Tr. 29-30.

[20] AE E.

• Personal Use: You are permitted to use [company] wireless devices for incidental personal activities, provided you follow the *prohibitions on accessing pornography*, gambling, etc. . . . (Appendix A, section 2.7.) (Emphasis added.)

Law and Policies

"[N]o one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988). Individuals are eligible for access to classified information "only upon a finding that it is clearly consistent with the national interest" to authorize such access. E.O. 10865 § 2; SEAD-4, ¶ E.4.

When evaluating an applicant's eligibility for a security clearance, an administrative judge must consider the adjudicative guidelines. In addition to brief introductory explanations, the guidelines list potentially disqualifying and mitigating conditions. The guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, an administrative judge applies the guidelines in a commonsense manner, considering all available and reliable information, in arriving at a fair and impartial decision. SEAD-4, Appendix A, ¶¶ 2(c), 2(d).

Department Counsel must present evidence to establish controverted facts alleged in the SOR. Directive ¶ E3.1.14. Applicants are responsible for presenting "witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by the applicant or proven . . . and has the ultimate burden of persuasion as to obtaining a favorable clearance decision." Directive ¶ E3.1.15.

Administrative Judges are responsible for ensuring that an applicant receives fair notice of the issues raised, has a reasonable opportunity to litigate those issues, and is not subjected to unfair surprise. ISCR Case No. 12-01266 at 3 (App. Bd. Apr. 4, 2014). In resolving the ultimate question regarding an applicant's eligibility, "[a]ny doubt concerning personnel being considered for national security eligibility will be resolved in favor of the national security." SEAD-4, Appendix A, ¶ 2(b). *See also* SEAD-4, ¶ E.4. Moreover, the Supreme Court has held that officials making "security clearance determinations should err, if they must, on the side of denials." *Egan*, 484 U.S. at 531.

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. 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 an 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.

Discussion

Guideline M – Use of Information Technology

The security concern for 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.

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

(e) unauthorized use of any information technology system.

The guideline notes several conditions that could mitigate security concerns under AG ¶ 41. One is potentially applicable in this case:

(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.

Applicant admitted that he viewed pornography on his company laptop from December 2015 to December 2016. That does not, however, settle the issue. The SOR did not allege that viewing pornography on a company laptop violated company policy. Nor did the parties address the applicability of the company VPN Policy to pornography. Indeed, one of Applicant's defenses was that until his viewing was discovered, he was unaware that such conduct violated company policy. The VPN Policy, however, has a clear, express prohibition on accessing pornography using company devices. Therefore, disqualifying condition AG ¶ 40(e) is triggered. The question is whether the security concern it implicates is mitigated.

There are a number of extenuating circumstances working in Applicant's favor. First, he has been employed by his current employer since 1991. Not only is that rare in the defense industry, it speaks to the high value his employer places on Applicant's work. Second, Applicant's past four years of performance evaluations have been stellar. Third, Applicant's four character affidavits were written by individuals who have known him personally and professionally for 10 years or more and who had read the SOR. They speak highly of his reliability, integrity, and trustworthiness. Fourth, at the time, two very close family members had died. Applicant felt deep sorrow for that loss. Fifth, he was also dealing with his own demanding career and with his diabetic condition. Sixth, there were

problems with his marriage, which Applicant and his spouse were addressing. Even before the SOR was issued (in October 2017), of his own volition, Applicant began weekly counseling sessions with a clinical therapist in March 2017. Her diagnosis is that he has no mental health disorder, and her prognosis is that Applicant will not revert to viewing pornography. Finally, an independent examination by a licensed psychologist found no basis for any mental health diagnosis and that Applicant is not addicted to pornography.

The picture that emerges is a concatenation of circumstances that overtaxed Applicant's judgment, and for a year (after more than 30 years as a professional), he resorted to pornography for relief. It was not secret or hidden from his wife or two adult children. Such a chain of circumstances is so unusual that it is unlikely to recur, and this episode does not cast doubt on Applicant's reliability, trustworthiness, or good judgment. AG ¶ 41(a) applies. I find in favor of Applicant on SOR ¶ 1.a.

SOR ¶ 1.b alleged that Applicant violated company policy by using his company laptop using his home network instead of his employer's network. Applicant denied that allegation, thereby putting the burden on the Government to prove that allegation. The VPN Policy addresses those instances when an employee is away from the home office. In those cases, the Policy counsels employees that they may use "all forms of wireless communication devices." It goes on to make four recommendations. The first recommendation is to connect "to known, password-protected networks where possible." That is exactly what Applicant did – he connected to his home network, which is password-protected. In plain English, to "recommend" something does not mandate it. In fact, when the VPN Policy wanted to mandate something, it did so clearly by prohibiting the accessing of pornography. It did not mandate the use of the company VPN when employees were out of the office. It merely recommended that. The Government has not met its burden proof. I find in favor of Applicant on SOR ¶ 1.b.

Applicant's testimony was thoughtful, candid, and credible, often on a difficult subject. The record does not raise doubts about Applicant's reliability, trustworthiness, good judgment, and ability to protect classified information. In reaching this conclusion, I weighed the evidence as a whole and considered if the favorable evidence outweighed the unfavorable evidence or *vice versa*. I also gave due consideration to the whole-person concept.[21] Accordingly, I conclude that Applicant met his ultimate burden of persuasion to show that it is clearly consistent with the national interest to grant him eligibility for 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 (Information Technology): For Applicant

[21] AG ¶ 2(a)(1)-(9). *See also*, ISCR Case No. 17-00506 at 3 (Aug. 7, 2018) (Administrative Judges must consider the evidence as a whole and not in an isolated or piecemeal fashion).

Subparagraphs 1.a-1.b: For Applicant

Conclusion

In light of the record as a whole, it is clearly consistent with the national interest to grant Applicant access to classified information.

Philip J. Katauskas
Administrative Judge