DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	
[NAME REDACTED]	)	ISCR Case No. 19-01084
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Eric Price, Esq., Department Counsel
For Applicant: Alan Edmunds, Esq.

05/26/2020

_____

Decision

_____

MALONE, Matthew E., Administrative Judge:

The security concerns raised by Applicant's misuse of his employer's laptop in violation of company policies are not mitigated. His request for a security clearance is denied.

Statement of the Case

On April 12, 2017, Applicant submitted an Electronic Questionnaire for Investigations Processing (e-QIP) to obtain eligibility for a security clearance required for his employment with a federal contractor. Based on the results of the ensuing background investigation, Department of Defense (DOD) adjudicators could not determine that it is clearly consistent with the interests of national security for Applicant to have a security clearance, as required by Security Executive Agent Directive (SEAD) 4, Section E.4, and by DOD Directive 5220.6, as amended (Directive), Section 4.2.

On May 17, 2019, DOD issued a Statement of Reasons (SOR) alleging facts that raise security concerns articulated in the adjudicative guidelines (AG) issued by the Director of National Intelligence on December 10, 2016, to be effective for all adjudications on or after June 8, 2017. Specifically, this case is governed by Guideline E (Personal Conduct) and Guideline M (Use of Information Technology).

Applicant timely responded to the SOR (Answer) and requested a hearing. With his response, he proffered Applicant's Exhibits (AX) A – I. I received the case on November 25, 2019, and convened the requested hearing on January 30, 2020. Department Counsel proffered Government Exhibits (GX) 1 – 4. Applicant appeared as scheduled, testified, and proffered AX J – Q. All exhibits were admitted without objection. I received a transcript of the hearing (Tr.) on February 10, 2020.

Procedural Note

AX Q is a report from a licensed clinical social worker (LCSW) who conducted an on-line evaluation of Applicant on January 29, 2020. The author also is a certified substance abuse counselor (CSAC), a master addiction counselor (MAC), and a substance abuse professional (SAP). In her report, she made certain clinical findings about possible mental health disorders Applicant may have had. In so doing, the LCSW also referenced the disqualifying and mitigating factors listed under Guideline D (Sexual Behavior), which is not at issue in this case, and she presented certain observations and conclusions about Applicant's suitability for a security clearance. (AX Q at page 5) I have considered the author's qualifications and her clinical findings as part of the record evidence as a whole. However, her qualifications do not include experience in the adjudication of DOD security clearance matters. Even had she established such qualifications, in DOHA proceedings the ultimate conclusion about an individual's suitability to have access to sensitive information is the sole province of the administrative judge. Accordingly, I have not considered the author's specific conclusions about Applicant's suitability for access to classified information.

Findings of Fact

Under Guideline M, the Government alleged that in November 2016, Applicant was fired for using a company laptop to view pornography between June and November 2016, in violation of his employer's policy for acceptable use of company information technology (SOR 1.a). This conduct was cross-alleged as adverse personal conduct under Guideline E (SOR 1.b). In response to the SOR, Applicant denied, with explanations, both SOR allegations. (Tr. 8 – 9) In addition to the facts established by Applicant's admissions, I make the following findings of fact.

Applicant is 46 years old and employed since January 2019 as a program manager for a defense contractor. He served on active duty in the United States Marine Corps between 1993 and 1995, when he was honorably discharged after becoming physical unable to serve any longer. Thereafter, Applicant worked and attended college, earning

an associate's degree in 1999 and a bachelor's degree in 2003. In August 2012, he earned a master's degree. (Answer; GX 1; AX F)

Applicant and his wife have been married since 2005 and have two children under the age of 10. His wife also works for the same defense contractor (Company A) where Applicant was employed between May 2015 and November 2016 as a project manager. (GX 1; Tr. 25 – 26)

Applicant has worked in the defense industry since 2003 for five companies including Company A. He first received an industrial security clearance in 2004. Throughout his career, Applicant has received training, usually on an annual basis, on a variety of security-related topics. Company A records show that on June 1, 2016, he acknowledged receiving training in cyber security and on Company A policies regarding the proper use of company computers and information technology systems. (GX 1; GX 4; Tr. 8)

On June 8, 2016, Applicant accessed a pornographic website from his company computer while at his permanent worksite and while connected to the company network. This occurred when Applicant connected a personally-owned external hard drive to his company computer. During a subject interview in September 2018, and in response to the SOR, Applicant claimed that while reviewing the files stored on that hard drive, he *inadvertently* clicked on the link for a pornographic website and that this was an isolated incident. Although Applicant was allowed to connect the hard drive to his work computer, accessing that website was a violation of company policy. When he clicked on the link, a security notice appeared on his screen advising him that he had been detected "making repeated attempts to visit improper websites with a classification branded for inappropriate material." The incident occurred on a Wednesday, but Applicant's supervisor was not in the office until the following Monday, June 13. Applicant claims he told his supervisor that day of the incident and that it was an inadvertent, one-time event. He further claimed that his supervisor did not formally counsel him, but advised Applicant to avoid such websites in the future. Applicant interpreted management's response as tacit permission to his use of pornography sites, even on a company laptop, as long as it was not during work hours or while connected to a company network. On Tuesday, June 14, 2016, the manager of the Company A information security department notified Applicant that he again had been detected accessing inappropriate sites on his company computer on Monday, June 13, 2016, the same day he purportedly self-reported his earlier conduct to his supervisor. Applicant's supervisor also was advised of this and Applicant was warned that "continued inappropriate activity will initiate a full security investigation, possible seizure of [his company laptop] for forensic analysis, and further report (sic) to HR and the Information Systems Security Officer." Applicant was also provided with a link to Company A's "Security Information Technology Acceptable Use Policy." (Answer; GX 1 – 4; Tr. 26 – 29, 32 – 33)

Applicant continued to view pornography using his Company A laptop on at least three other occasions between June 2016 and November 2016. Applicant admits doing

so, but he insisted that he was off-duty each time and was not connected to the company information network when he accessed pornography sites. Applicant has further claimed that he was not made aware of the Company A policy against using the laptop in that way. Most of Applicant's conduct in this regard occurred while Applicant was away from home on work-related travel overseas. Despite this, Company A's information security organization detected numerous websites and an extensive level of activity, some of which involved sites that reflected an interest in underage girls. Applicant denied that he ever viewed child pornography. He acknowledged that he has viewed pornography for several years. The LCSW evaluation on January 29, 2020 found no disorder or compulsion associated with Applicant's conduct. Applicant has also acknowledged that he understands the cyber security vulnerabilities that can arise when one accesses websites such as those at issue here. He insists that he has learned his lesson, and his wife has stated her confidence that Applicant no longer views pornography. (GX 1 – 4; AX P; AX Q; Tr. 26 – 30, 47 – 57)

Applicant presented five character reference letters, four of which indicated Applicant had disclosed the reasons why his security clearance eligibility was in doubt. It is not apparent, however, that Applicant disclosed all of the facts about his misuse of a company laptop to view pornography. He also presented information that shows he has been an excellent employee in terms of his performance and technical expertise. His current employer has, so far, given him positive feedback about his performance over the past year. (Answer; AX A – E; AX G; AX H; AX N; AX O)

Policies

Each security clearance decision must be a fair, impartial, and commonsense determination based on examination of all available relevant and material information, and consideration of the pertinent criteria and adjudication policy in the adjudicative guidelines (AG). (*See* Directive, 6.3) Decisions must also reflect consideration of the factors listed in ¶ 2(d) of the guidelines. Commonly referred to as the "whole-person" concept, those factors are:

> (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.

The presence or absence of a disqualifying or mitigating condition is not determinative of a conclusion for or against an applicant. However, specific applicable guidelines should be followed whenever a case can be measured against them as they represent policy guidance governing the grant or denial of access to classified

information. A security clearance decision is intended only to resolve whether it is clearly consistent with the national interest for an applicant to either receive or continue to have access to classified information. (Department of the Navy v. Egan, 484 U.S. 518 (1988))

The Government bears the initial burden of producing admissible information on which it based the preliminary decision to deny or revoke a security clearance for an applicant. Additionally, the Government must be able to prove controverted facts alleged in the SOR. If the Government meets its burden, it then falls to the applicant to refute, extenuate or mitigate the Government's case. Because no one has a "right" to a security clearance, an applicant bears a heavy burden of persuasion. (*See* Egan, 484 U.S. at 528, 531) A person who has access to classified information enters into a fiduciary relationship with the Government based on trust and confidence. Thus, the Government has a compelling interest in ensuring each applicant possesses the requisite judgment, reliability and trustworthiness of one who will protect the national interests as his or her own. The "clearly consistent with the national interest" standard compels resolution of any reasonable doubt about an applicant's suitability for access in favor of the Government. (*See* Egan; AG ¶ 2(b))

Analysis

Use of Information Technology

The security concern under this guideline is stated at 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 record evidence as a whole shows that Applicant repeatedly violated Company A policies regarding acceptable use of his company laptop. He did so with full knowledge of those policies within days of receiving company training on that subject. He also repeated his behavior after being specifically warned that such conduct would have significant consequences if he persisted. He eventually lost his job as a result of his misconduct. This information is most directly addressed in the first sentence of AG ¶ 39, above, but also requires application of AG ¶ 40(g) (*negligence or lax security practices in handling information technology that persists despite counseling by management*).

I also have considered the following AG ¶ 41 mitigating conditions:

> (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;
>
> (b) the misuse was minor and done solely in the interest of organizational efficiency and effectiveness;
>
> (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.

The events at issue occurred nearly four years ago and Applicant claims he has learned his lesson about the need to properly use information technology. He also now acknowledges that he acted as alleged in the SOR; however, in response to the SOR and at his hearing, he stated that he was not properly trained or advised about Company A policies or the security concerns posed by accessing pornographic websites. These claims are directly at odds with the persuasive information contained in Company A records about these events. Applicant's testimony was not credible, and his inconsistent statements about his conduct undermine confidence that his past conduct no longer casts doubt on his judgment and reliability. The AG ¶ 41 mitigating conditions cited above are not applicable and the security concerns under this guideline are not mitigated.

Personal Conduct

The security concern under this guideline is stated, in relevant part, at AG ¶ 15:

> 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 or sensitive information.

Applicant violated Company A policies about the use of his company laptop. He did so despite knowing it was against company policy and after being warned that continued violations would result in serious consequences. When Applicant told his boss about the June 8 incident, he misled him by saying his access was a one-time inadvertent event; however, the day he had that conversation with his boss, he repeated his misconduct and was more formally cautioned against future misuse of his laptop. Available information shows Applicant continued his misconduct for the next five months until he was fired. He was given several opportunities to correct his behavior, which he failed to do. This information requires application of AG ¶ 16(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.
>
> I also have considered the following AG ¶ 17 mitigating conditions:
>
> (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; and
>
> (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.

During his background investigation, in his response to the SOR, and at his hearing, Applicant again claimed that his access was either inadvertent or was somehow acceptable. The weight of these claims shows that he has not been candid about what he did and that he has not yet accepted responsibility for his actions at Company A. Even in the absence of similar conduct over the past four years, Applicant's inconsistent response to the security concerns reasonably raised by this information continues to undermine confidence in his judgment and reliability. The AG ¶ 17 mitigating conditions cited above cannot be applied here, and the security concerns raised under this guideline are not mitigated.

I also evaluated this record in the context of the whole-person factors listed in AG ¶ 2(d). I particularly note the value of Applicant's military service and the positive information about his work in the defense industry. Nonetheless, Applicant's inconsistent testimony about his conduct creates persistent doubts about his judgment and reliability. Because protection of the interests of national security is the principal focus of these adjudications, those doubts must be resolved against the Applicant's request for clearance.

Formal Findings

Formal findings 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:	Against Applicant
Paragraph 2, Guideline E:	AGAINST APPLICANT
Subparagraph 2.a:	Against Applicant

Conclusion

It is not clearly consistent with the interests of national security for Applicant to have access to classified information. Applicant's request for a security clearance is denied.

MATTHEW E. MALONE
Administrative Judge