DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 19-01753
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Andre M. Gregorian, Esq., Department Counsel
For Applicant: *Pro se*

02/14/2020

_____

Decision

_____

HARVEY, Mark, Administrative Judge:

Applicant viewed pornographic images on government and employer-owned computers intermittently from 1998 to 2018. He mitigated Guideline D (sexual behavior) security concerns, and he refuted Guideline E (personal conduct) security concerns. However, Guideline M (use of information technology) security concerns are not mitigated. Access to classified information is denied.

Statement of the Case

On October 4, 2007, and September 26, 2018, Applicant completed and signed Questionnaires for National Security Positions (SF 86) or security clearance applications (SCA). (Government Exhibit (GE) 1; GE 2) On June 26, 2019, the Department of Defense (DOD) Consolidated Adjudications Facility (CAF) issued a statement of reasons (SOR) to Applicant under Executive Order (Exec. Or.) 10865, *Safeguarding Classified Information within Industry*, February 20, 1960; DOD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (Directive), January 2, 1992; and Security Executive Agent Directive 4, establishing in Appendix A the *National Security Adjudicative Guidelines for Determining Eligibility for Access to Classified Information or Eligibility to Hold a Sensitive Position* (AGs), effective June 8, 2017. (Hearing Exhibit (HE) 2)

The SOR detailed reasons why the DOD CAF did not find under the Directive that it is clearly consistent with the interests of national security to grant or continue a security

clearance for Applicant and recommended referral to an administrative judge to determine whether a clearance should be granted, continued, denied, or revoked. Specifically, the SOR set forth security concerns arising under Guidelines D, M, and E. (HE 2) On July 31, 2019, Applicant responded to the SOR and requested a hearing. (HE 3)

On December 23, 2019, Department Counsel was ready to proceed. On December 30, 2019, the case was assigned to me. On December 30, 2019, the Defense Office of Hearings and Appeals (DOHA) issued a notice of hearing, setting the hearing for January 23, 2020. (HE 1) Applicant's hearing was held as scheduled.

During the hearing, Department Counsel offered four exhibits; Applicant offered two exhibits; and all proffered exhibits were admitted into evidence without objection. (Tr. 14-15, 20-22; GE 1-4; Applicant Exhibit (AE) A-AE B). On January 31, 2020, DOHA received a transcript of the hearing.

Some details were excluded to protect Applicant's right to privacy. Specific information is available in the cited exhibits and transcript pages.

Findings of Fact

In Applicant's SOR response, he admitted all of the SOR allegations. (HE 3) He also provided extenuating and mitigating information. Applicant's admissions are accepted as findings of fact. Additional findings of fact follow.

Applicant is a 55-year-old communication system engineer, who was employed by a DOD contractor from September 2007 to August 2018. (Tr. 6, 23, 25-26; GE 1) He was recently hired by another DOD contractor. In 1987, he was commissioned in the Air Force. (Tr. 8) He was deployed to Afghanistan from August 2005 to January 2006. (Tr. 9) His Air Force specialty was information technology communications. (Tr. 10) In 2007, he retired from the Air Force as a lieutenant colonel. (Tr. 8, 23) His highest award was the Joint Service Commendation Medal. (Tr. 9) He held a security clearance continuously since 1987 when he joined the Air Force. (Tr. 23-24) In 2013, he was granted access to sensitive compartmented information (SCI). (Tr. 24)

In 1983, Applicant graduated from high school, and in 1987, he received a bachelor's degree with a major in electrical engineering. (Tr. 7; GE 1) In 1994, he received his first master's degree in information systems; in 2002, he received his second master's degree in military operational art and science; and in 2016, he received his third master's degree in science and religion. (Tr. 7-8; GE 1) In 1998, he married and his two step children are ages 34 and 38. (Tr. 12)

Sexual Behavior, Use of Information Technology, and Personal Conduct

SOR ¶¶ 2 (use of information technology) and 3 (personal conduct) cross-allege conduct that is alleged in SOR ¶ 1 (sexual behavior).

SOR ¶ 1.c alleges Applicant received verbal counseling on at least two occasions for viewing pornographic websites from August 1998 to July 2001. (Tr. 34) On about two or three occasions, he used his government-owned desktop computer in his Air Force office to access pornographic websites for 10 to 15 minutes on each occasion. (Tr. 35-36, 75; GE 3) It was at the end of the duty day. (Tr. 35) He did not intentionally download any pornography on his computer. (Tr. 38) He was verbally counseled and told to stop accessing pornographic websites with his government computer. (Tr. 38) The first counseling did not seem to be with serious intent. (Tr. 39) "It was given to me with like a wink" with an instruction to "knock it off." (Tr. 39) The policy against using a government computer to access pornography was informal and not well developed at that time. (Tr. 39-40) He acknowledged that his computer had access to sensitive information, and his actions could have compromised that information technology system by exposing it to viruses and malware. (Tr. 41) At the time he was accessing the pornographic sites, he was not thinking about the risk to sensitive information. (Tr. 41)

SOR ¶ 1.b alleges Applicant received a letter of reprimand in about October 2004 while serving on active duty for misuse of a government computer. (Tr. 42) He admitted that he accessed pornographic websites on a government-issued computer. (Tr. 42) The computer he used was a Morale, Welfare, and Recreation (MWR) computer that was in a break area. (Tr. 32) The MWR computer was for general access to enable Air Force employees to access their email, and the MWR computer was not assigned to Applicant. (Tr. 42) He went to two or three pornographic websites over the course of one day in September 2004. (Tr. 42-43) He did not intentionally download any pornography on the MWR computer. (Tr. 38) His computer misuse was detected through a computer log that was used to monitor the computer's use. (Tr. 44) There was no evidence that the pornography was downloaded or saved on the MWR computer. (Tr. 45) In 2004, he viewed pornography at home on an infrequent basis. (Tr. 46) He received some counseling from a licensed counselor to address his pornography issue; however, it was ineffective. (Tr. 47) The letter of reprimand was for violation of a regulation under Article 92, Uniform Code of Military Justice (UCMJ). *See. e.g.,* DOD Regulation 5500.7-R, *Joint Ethics Regulation*, (Aug. 30, 1993), ¶ 2-301(2)(d). The reprimand adversely affected his future assignments, and he was not selected for promotion to colonel. (Tr. 73) During his November 7, 2007, Office of Personnel Management personal subject interview, Applicant said he learned his lesson about misuse of government computers after his reprimand in 2004. (Tr. 49; GE 3)

SOR ¶ 1.a alleges Applicant used an employer-owned computer to view pornographic websites from about January 2018 to about July 2018. He resigned in lieu of being terminated by his employer for this misuse of his employer's computer. He viewed the pornography in his employer's building in a conference room. (Tr. 50, 55) He turned off the virtual private network (VPN) connection to circumvent or bypass his employer's firewall. (Tr. 59) Switching off the VPN enabled him to access sites his employer would normally block. (Tr. 59) He acknowledged that by turning off the VPN he engaged in "unauthorized manipulation of an information system." (Tr. 59) He also deleted the search logs after he went to the pornographic websites. (Tr. 72)

Applicant viewed pornography once or twice a month using his employer's computer, and he accessed the sites for one or two hours at a time. (Tr. 50; GE 3) He accessed the sites during lunchtime or when things were slow at the office. (Tr. 51; GE 3) He estimated that he downloaded about 1,000 pictures but no videos, and he deleted the pictures within 24 hours after downloading them. (Tr. 53-54) His employer did not find any pornography on the computer he used to access pornographic websites. (Tr. 59) He said the computer he misused did not directly affect DOD. (Tr. 30) His employer's computer did not directly access a DOD network; however, this computer did access his employer's network. (Tr. 30-31) His misuse of his employer's computer violated his employer's policies and procedures. (Tr. 58) He committed multiple infractions because after he misused his employer's computer the first time, and nothing happened, he did not believe his employer was serious about enforcement of prohibitions against accessing pornography on his employer's computers. (Tr. 55-57) He resigned from his employment because he believed it was likely that he would be fired. (Tr. 57)

Applicant received routine annual briefings on security and information systems. (Tr. 32-33) Throughout his career, Applicant was aware that he was not permitted to access pornography websites or view pornography using government or his employer's computers. (Tr. 31-32) He viewed pornographic websites for pleasure. (Tr. 36) He became sexually aroused; however, he did not masturbate while viewing the pornography. (Tr. 37, 52) He did not view child pornography. (Tr. 38) He conceded that in the past he had a problem with or addiction to pornography. (Tr. 46-47) Applicant infrequently viewed pornography on his home computer from 2004 to 2018. (Tr. 49)

Theoretically, when Applicant downloaded a pornographic picture onto his employer's computer, that picture might have contained a virus that could be transferred onto his employer's network. (Tr. 75-76) The virus could be transferred via his employer's network onto a Microsoft Word document or PowerPoint presentation, and in turn, when these items were sent to the DOD, the virus could be downloaded onto the DOD network. (Tr. 75-76) Applicant was not thinking about possible penetration of security or creation of a "backdoor" into the DOD network when he was looking at pornography or visiting pornographic websites using his employer's computer. (Tr. 77)

Applicant reluctantly conceded that in the past he was "addicted" to pornography. (Tr. 70) His viewing of pornography was a choice, and ultimately, he had the power or free will and could choose not to view pornography. (Tr. 70) He said that in the past he had a compulsion to view pornography, and he "fell into a bondage area." (Tr. 70)

Applicant met with his pastor on a weekly basis from August 2018 to about March 2019, and less frequently thereafter for counseling to help with his pornography issue. (Tr. 62-66; SOR response) After July 2018, Applicant viewed pornography on his home computer on only one occasion. (Tr. 61) He disclosed this viewing to his spouse and pastor. (Tr. 61) Occasionally his spouse attended the meetings with his pastor. (Tr. 64) His spouse has complete knowledge of his issue with pornography. (Tr. 64) Applicant disclosed his misuse of computers involving pornography to security, coworkers, friends, people at church, and family. (Tr. 60, 66; GE 3) He was not worried about public disclosure of his past problem with pornography because of his success in his endeavors

to stop viewing pornography. (Tr. 67-68) He expressed his remorse for his involvement with pornography. (Tr. 83)

Character Evidence

A GS-15, who has known Applicant for 14 years in a professional capacity, described Applicant as having excellent integrity and loyalty. (SOR response) His statement supported Applicant's access to classified information. (*Id*.) In 2019, he received an annual merit increase and spot bonus increase from his employer for his hard work. (AE B)

Applicant's pastor has provided counseling to Applicant since July 2018. (SOR response) He said Applicant is "remorseful, repentant, and stands in low probability of improperly using any PC or network again." (*Id*.) He recommended mitigation of Applicant's issues. (*Id*.)

Applicant described himself as patriotic and loyal to the government. (Tr. 77) "[T]here were no security incidents" during his decades of government service. (Tr. 77)

Policies

The U.S. Supreme Court has recognized the substantial discretion of the Executive Branch in regulating access to information pertaining to national security emphasizing, "no one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988). As Commander in Chief, the President has the authority to control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to have access to such information." *Id*. at 527. The President has authorized the Secretary of Defense or his designee to grant applicant's eligibility for access to classified information "only upon a finding that it is clearly consistent with the national interest to do so." Exec. Or. 10865.

Eligibility for a security clearance is predicated upon the applicant meeting the criteria contained in the adjudicative guidelines. These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, these guidelines are applied in conjunction with an evaluation of the whole person. An administrative judge's overarching adjudicative goal is a fair, impartial, and commonsense decision. An administrative judge must consider all available, reliable information about the person, past and present, favorable and unfavorable.

The Government reposes a high degree of trust and confidence in persons with access to classified information. This relationship transcends normal duty hours and endures throughout off-duty hours. 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 about potential, rather than actual, risk of compromise of classified information. Clearance decisions must be "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." *See* Exec. Or. 10865 § 7.

Thus, nothing in this decision should be construed to suggest that it is based, in whole or in part, on any express or implied determination about applicant's allegiance, loyalty, or patriotism. It is merely an indication the applicant has not met the strict guidelines the President, Secretary of Defense, and DNI have established for issuing a clearance.

Initially, the Government must establish, by substantial evidence, conditions in the personal or professional history of the applicant that may disqualify the applicant from being eligible for access to classified information. The Government has the burden of establishing controverted facts alleged in the SOR. *See Egan*, 484 U.S. at 531. "Substantial evidence" is "more than a scintilla but less than a preponderance." *See v. Washington Metro. Area Transit Auth.*, 36 F.3d 375, 380 (4th Cir. 1994). The guidelines presume a nexus or rational connection between proven conduct under any of the criteria listed therein and an applicant's security suitability. *See* ISCR Case No. 95-0611 at 2 (App. Bd. May 2, 1996).

Once the Government establishes a disqualifying condition by substantial evidence, the burden shifts to the applicant to rebut, explain, extenuate, or mitigate the facts. Directive ¶ E3.1.15. An applicant "has the ultimate burden of demonstrating that it is clearly consistent with the national interest to grant or continue his security clearance." ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002). The burden of disproving a mitigating condition never shifts to the Government. *See* ISCR Case No. 02-31154 at 5 (App. Bd. Sep. 22, 2005). "[S]ecurity clearance determinations should err, if they must, on the side of denials." *Egan*, 484 U.S. at 531; *see* AG ¶ 2(b).

Analysis

Sexual Behavior

AG ¶ 12 contains the security concern for sexual behavior:

> Sexual behavior that involves a criminal offense; reflects a lack of judgment or discretion; or may subject the individual to undue influence of coercion, exploitation, or duress. These issues, together or individually, may raise questions about an individual's judgment, reliability, trustworthiness, and ability to protect classified or sensitive information. Sexual behavior includes conduct occurring in person or via audio, visual, electronic, or written transmission. No adverse inference concerning the standards in this Guideline may be raised solely on the basis of the sexual orientation of the individual.

AG ¶ 13 includes conditions that could raise a security concern and may be disqualifying in this case:

> (a) sexual behavior of a criminal nature, whether or not the individual has been prosecuted;

(b) a pattern of compulsive, self-destructive, or high-risk sexual behavior that the individual is unable to stop;

(c) sexual behavior that causes an individual to be vulnerable to coercion, exploitation, or duress; and

(d) sexual behavior of a public nature or that reflects lack of discretion or judgment.

The record evidence establishes AG ¶¶ 13(a) and 13(d); however, the other disqualifying conditions do not apply. When he viewed pornography on his government computer, he was on active duty, and he violated a regulation and Article 92, UCMJ. There was no evidence that viewing pornography on his employer's computer was a crime. He disclosed his involvement with pornography. Applicant was able to stop viewing pornography. AG ¶¶ 13(b) and 13(c) are not established. His repeated access to pornography with a government or employer-owned computer reflected a lack of discretion and judgment.

The DOHA Appeal Board concisely explained Applicant's responsibility for proving the applicability of mitigating conditions as follows:

> Once a concern arises regarding an Applicant's security clearance eligibility, there is a strong presumption against the grant or maintenance of a security clearance. *See Dorfmont v. Brown*, 913 F. 2d 1399, 1401 (9th Cir. 1990), *cert. denied*, 499 U.S. 905 (1991). After the Government presents evidence raising security concerns, the burden shifts to the applicant to rebut or mitigate those concerns. *See* Directive ¶ E3.1.15. The standard applicable in security clearance decisions is that articulated in *Egan*, *supra*. "Any doubt concerning personnel being considered for access to classified information will be resolved in favor of the national security." Directive, Enclosure 2 ¶ 2(b).

ISCR Case No. 10-04641 at 4 (App. Bd. Sept. 24, 2013).

AG ¶ 14 lists conditions that could mitigate security concerns:

(a) the behavior occurred prior to or during adolescence and there is no evidence of subsequent conduct of a similar nature;

(b) the sexual behavior happened so long ago, so infrequently, or under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or judgment;

(c) the behavior no longer serves as a basis for coercion, exploitation, or duress;

(d) the sexual behavior is strictly private, consensual, and discreet; and

(e) the individual has successfully completed an appropriate program of treatment, or is currently enrolled in one, has demonstrated ongoing and consistent compliance with the treatment plan, and/or has received a favorable prognosis from a qualified mental health professional indicating the behavior is readily controllable with treatment.

Applicant's private viewing of adult pornography on a personal laptop computer or other personally-owned media outside the workplace is protected conduct under the First Amendment and the liberty interest of the Due Process Clause of the Fourteenth Amendment to the U.S. Constitution. *See Lawrence v. Texas*, 539 U.S. 558 (2003)(discussing right to engage in private, consensual sexual behavior); *United States v. Playboy Entertainment Group, Inc.*, 529 U.S. 803 (2000) (discussing adult pornography and First Amendment). His sexual behavior involving viewing adult pornography in the privacy of his home does not cast doubt on his current reliability, trustworthiness, and good judgment.

AG ¶ 14(c) applies. Applicant has widely disclosed his history of involvement with pornography, and it does not constitute a basis for coercion, exploitation, or duress. He has not viewed pornography on his employer's computer since July 2018 demonstrating he has the ability to refrain from viewing pornography in an inappropriate or prohibited context. Guideline D security concerns are mitigated.

Use of Information Technology

AG ¶ 39 articulates the security concern for use of information technology:

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 including:

(a) unauthorized entry into any information technology system;

(b) unauthorized modification, destruction, or manipulation of, or denial of access to, an information technology system or any data in such a system;

(c) use of any information technology system to gain unauthorized access to another system or to a compartmented area within the same system;

(d) downloading, storing, or transmitting classified, sensitive, proprietary, or other protected information on or to any unauthorized information technology system;

(e) unauthorized use of any information technology system;

(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;

(g) negligence or lax security practices in handling information technology that persists despite counseling by management; and

(h) any misuse of information technology, whether deliberate or negligent, that results in damage to the national security.

AG ¶¶ 40(b), 40(e), 40(f), and 40(g) apply. Applicant downloaded pornography onto his employer-owned computer. He turned off the VPN connection to circumvent or bypass his employer's firewall. This enabled him to access sites his employer would normally block, and constituted an unauthorized manipulation of an information system. When he was an active duty Air Force officer, he was counseled twice about not using his government computer to view pornography. He subsequently received a letter of reprimand for viewing pornography using an MWR computer. He viewed pornography using his employer's computer in 2018. He was well aware from his information technology education, background, and training that he was not permitted to view pornography on a government or employer-owned computer.

AG ¶ 41 lists conditions that could mitigate security concerns as follows:

(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.

None of the mitigating conditions apply. Applicant has a lengthy history and repeated violations of policies governing use of government and employer computers. His misuse of his employer's computer in 2018 is relatively recent. He knew viewing

pornography using a government computer and his employer's computer was improper, and he did it anyway. He knew going to untrustworthy websites could compromise a computer system. There were efforts in 2018 to conceal that activity by deleting the logs. Use of information technology security concerns are not mitigated.

Personal Conduct

AG ¶ 15 explains why personal conduct is a security concern stating:

> 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 includes conditions that could raise a security concern and may be disqualifying in this case:

> (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; 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.

As indicated, in the use of information technology section, *supra*, there is sufficient evidence for an adverse determination under Guideline M. Moreover, his misuse of a government computer and his employer's computer is explicitly covered under Guideline M. Applicant has widely disclosed his history of misuse of computers and his involvement

with pornography. He is not "vulnerab[le] to exploitation, manipulation, or duress by a foreign intelligence entity or other individual or group." I am confident he would report to security officials any attempt by a foreign intelligence entity to exploit him because of his history of misuse of computers. He has refuted security concerns under Guideline E.

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), "[t]he ultimate determination" of whether to grant a security clearance "must be an overall commonsense judgment based upon careful consideration of the guidelines" and the whole-person concept. My comments under Guidelines D, M, and E are incorporated in my whole-person analysis. Some of the factors in AG ¶ 2(d) were addressed under those guidelines but some warrant additional comment.

Applicant is a 55-year-old communication system engineer, who was employed by a DOD contractor from September 2007 to August 2018. He was recently hired by another DOD contractor. He served as an active duty Air Force officer from 1987 to 2007. He was deployed to Afghanistan from August 2005 to January 2006. His Air Force specialty was information technology communications. He honorably retired from the Air Force as a lieutenant colonel. His highest award was the Joint Service Commendation Medal. He held a security clearance continuously since 1987 when he joined the Air Force. Applicant has three master's degrees.

There is no evidence that Applicant improperly disclosed classified information. He described himself as a loyal patriotic American. His promotion to lieutenant colonel, deployment to a combat zone, honorable retirement from the Air Force, and 13 years of dedicated employment by government contractors demonstrate a 32-year track record of contributions to the national defense. *See* ISCR Case No. 18-02581 at 4 (App. Bd. Jan. 14, 2020) (noting admissibility of "good security record," and commenting that security concerns may nevertheless not be mitigated). At his hearing and during OPM interviews, he candidly and honestly admitted his multiple instances of misuse of government and contractor-owned computers. His detailed and candid descriptions of his pornography-related conduct and efforts to terminate his involvement with pornography are important steps on the road to rehabilitation.

The weight of the evidence is against access to classified information for Applicant at this time. Prior to July 2001, Applicant was verbally counseled twice and told not to use a government-owned computer to view pornography. In 2004, he received a letter of reprimand for using an MWR computer to view pornography. In 2018, he viewed pornography on his employer's computer on multiple occasions. His actions to bypass security to access pornography, his deletion of digital evidence that he accessed pornography, and his history of addiction to pornography increase security concerns. His misuse was detected through security measures; however, once his misuse was discovered, he voluntarily disclosed additional negative pornography-related computer misuse.

It is well settled that once a concern arises regarding an applicant's security clearance eligibility, there is a strong presumption against the granting a security clearance. *See Dorfmont*, 913 F. 2d at 1401. I have carefully applied the law, as set forth in *Egan,* Exec. Or. 10865, the Directive, and the AGs, to the facts and circumstances in the context of the whole person. Sexual behavior security concerns are mitigated, and personal conduct security concerns are refuted. Unmitigated use of information technology systems security concerns lead me to conclude that grant of a security clearance to Applicant is not warranted at this time.

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 D:	FOR APPLICANT
Subparagraphs 1.a through 1.c:	For Applicant
Paragraph 2, Guideline M:	AGAINST APPLICANT
Subparagraph 2.a:	Against Applicant
Paragraph 3, Guideline E:	FOR APPLICANT
Subparagraph 3.a:	For 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 or continue Applicant's eligibility for a security clearance. Eligibility for access to classified information is denied.

_____
Mark Harvey
Administrative Judge