DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 20-03502
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Andrew Henderson Esq., Department Counsel
For Applicant: Aileen Xenakis Kozlowski, Esq., Attorney At Law

November 10, 2022

_____

Decision

_____

Lokey Anderson, Darlene D., Administrative Judge:

Statement of the Case

On November 12, 2019, Applicant submitted a security clearance application (e-QIP). (Government Exhibit 1.) On December 28, 2021, the Department of Defense Consolidated Adjudications Facility (DoD CAF) issued Applicant a Statement of Reasons (SOR), detailing security concerns under Guideline D, Sexual Behavior; Guideline M, Use of Information Technology; and Guideline E, Personal Conduct. The action was taken 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) effective within the DoD after June 8, 2017.

Applicant answered the SOR on February 27, 2021, and requested a hearing before an administrative judge. The case was assigned to me on May 18, 2022. The Defense Office of Hearings and Appeals issued a notice of hearing on June 16, 2022,

and the hearing was convened as scheduled on August 10, 2022. The Government offered four exhibits, referred to as Government Exhibits 1 through 4, which were admitted without objection. The Applicant offered five exhibits, referred as Applicant's Exhibits A through E, which were admitted without objection. Applicant testified on his own behalf. DOHA received the transcript of the hearing (Tr.) on August 18, 2022.

Findings of Fact

Applicant is 44 years old. He is married with five children. He has a Master's degree in Electrical Engineering. He is employed by a defense contractor as a Design and Analysis Engineer IV. He is seeking to retain a security clearance in connection with his employment.

Guideline D – Sexual Behavior
Guideline M – Use of Information Technology
Guideline E – Personal Conduct

The SOR alleged that Applicant for many years, between 2003 and 2014, engaged in sexual misconduct in the workplace, the misuse of information technology, and poor personal conduct. Applicant admits in part and denies in part the allegations set forth in the SOR. (*See* Applicant's Answer to the SOR.)

Applicant's first job out of college was working for a defense contractor from 2003 to 2011. He was granted a security clearance in 2003 or 2004. During this period of employment, he engaged in many acts of misconduct. In 2009, he underwent a polygraph examination and admitted that he viewed pornography on his corporate computer about a dozen times, and he masturbated in his office on three to five occasions. (Tr. p. 49.) In September 2009, he was required to sign a Government policy statement confirming this misconduct. From 2011 to 2013, he left his employment in the defense industry and worked outside of the industry. (Government Exhibit 3.)

In 2013, Applicant re-entered the defense industry, and started working for his current employer. He was granted a special access clearance in late 2014. In 2014, he again underwent a polygraph examination. During this polygraph examination, Applicant admitted that he had relapsed in viewing pornography at work, which occurred about ten times. (Tr. p. 51.) This time, however, he was viewing pornography on his cell phone while at work. This misconduct occurred about every three months or so. He also admitted to misusing his corporate computer in many ways. He loading a non-work related compact disc into it between 2003 and 2007; he had used a personal USB drive to transfer proprietary text files and powerpoint presentations from 2008 to 2011; he had used a personal USB drive to transfer proprietary information between November 2013 to March 2014; and, he had used his corporate computer to charge his cell phone one to two times per week from October 2013 to May 2014. Applicant stated that he deliberately withheld information about his use of personal USB drives in his corporate computer during his earlier investigation in 2008. (Government Exhibit 3.)

1.a. Applicant, on multiple occasions between 2005 until at least 2014, used the corporate computer to view pornography at work. This conduct was in violation of company and DoD policies and regulations, as well as United States Intelligence Community policy. Applicant testified that in 2005, he was working full time for a defense contractor, and working on his Master's degree. He was twenty-five years old, newly married, with a young family. He was balancing lots of demands, and was stressed. He found that the only privacy he had was at the office, and he started to view pornography at work on the corporate computer. This misconduct continued until at least 2014. He explained that he would usually work more than the standard 40-hour work week, and after hours or on a break he would view pornography. He stated that he never did it where anyone could see him. He stated that he has not engaged in this misconduct since 2014. He knew this misconduct to be prohibited, but chose to engage in it anyway.

1.b. Applicant, on multiple occasions from 2005 until at least 2008, masturbated in his office while at work. He believes this occurred between two to four or five separate occasions. He testified that he realized that this behavior was not in line with his religious beliefs and wanting to be honest with his wife and his church leaders, and so he started seeing a counselor for this behavior. He stated that he has not engaged in this misconduct since 2008. Applicant knew this misconduct to be prohibited, but chose to engage in it anyway.

2.a. See Applicant's misconduct discussion above under 1.a.

2.b. Applicant, on multiple occasions from 2008 to at least 2014, transferred personal files without authorization between his corporate computer and his personal home computer using his personal thumb drives. He stated that he has not engaged in this misconduct since 2014. He knew this misconduct to be prohibited, but chose to engage in it anyway.

2.c. Applicant, on multiple occasions from about 2003 to 2007, loaded unauthorized software onto his corporate computer. He testified that he would load a music CD on his corporate computer. He also used the charger on his corporate computer to charge his personal cell phone. He stated that he has not engaged in this misconduct since 2007. He knew this misconduct to be prohibited, but chose to engage in it anyway.

3.a. In February 2015, the Government revoked Applicant's existing access to classified Information and disapproved any additional access for violation of Intelligence Community Policy guidance 704.2. In September 2009, Applicant signed a US Government policy statement wherein it noted that his viewing of pornography on his corporate computer, and his masturbating in the office, which occurred between 2005 to 2008 were noted misconduct under personal conduct and misuse of information technology systems. He understood at that time that his misconduct was against company and Government policies. In 2014, during polygraph testing of the Applicant, he stated that he did not take the signed policy statement seriously. He believed his misconduct was okay because he was not using his corporate computer. At that time,

he stated that he attended Sexaholics Anonymous due to his addiction to pornography. He estimated that he has occasion to relapse into the sexual addiction approximately every three months where he views pornography on his cell phone while at work. (Government Exhibit 3.)

3.b. See Applicant's misconduct discussed above in paragraph 1.

3.c. See Applicant's misconduct discussed above in paragraph 2.

Two polygraph examinations of the Applicant, the first conducted by a previous employer in 2008, and the second conducted in 2014, by his current employer, revealed that for many years, while employed in the defense industry, Applicant has engaged in sexual misconduct in the workplace. He has also misused information technology, and engaged in poor personal conduct. These actions were in violation of DoD policies and procedures.

Applicant testified that he has received regular security briefings from his employers since beginning his employment in the defense industry. (Tr. p. 76.) He stated that when he started working for the defense industry he was young and ignorant and just learning the rules and regulations. He believes that he now has a firm understanding of the company policy and procedures. He believes he has grown and matured since he committed these violations, as it has been nearly ten years. This is not entirely accurate. Applicant engaged in misconduct as a young man in his twenties, and this misconduct continued, with pattern of relapse, well into his late thirties. He underwent his first polygraph examination in 2008, and was made aware of misconduct, when he signed a U.S. Government policy statement in September 2009. His relapses were noted in 2014, and his Special Access was revoked in February 2015.

Applicant testified that although he would like to work in the defense industry for a contractor, he does not need a security clearance in order to be employable. He has chosen to confront these issues in his past and would like to work for the Government, but there are many companies outside of the Department of Defense that could use his skills without the need for a security clearance. In fact, that is what he was doing between 2011 and 2013, working in other fields outside of the Government.

Excerpts from Applicant's employment records reflect that he has been a major contributor to the company. Documents reflecting his job performance show that he has either "met expectations", "exceeded", or "far exceeded" his job requirements. He has also been eligible for the retention bonus program. (Applicant's Exhibit B.) Applicant testified that since 2013, his performance evaluations have been excellent. He has received ratings of either "exceeds expectations" or "greatly exceeds expectations." (Tr. p. 20.) He stated that he gets along well with his co-workers and management.

Letters of recommendation from various individuals who know the Applicant well, who include friends, church members, his wife, and his counselor, attest to his character, patriotism and ability to protect classified information. They collectively

indicate that Applicant is trustworthy, responsible and has good judgment. They all recommend that he be granted a security clearance. (Applicant's Exhibit C.)

A letter from his counselor confirmed that Applicant attended sessions twice a month at first and then later on a monthly basis. The sessions involved therapy in dealing with stress management techniques and how to avoid his addiction. In addition how to be accountable to his wife, church community and others. He believes that Applicant is committed to ensuring that his sexual misconduct does not continue.

Applicant is a very involved father who coaches his children's basketball, baseball, and soccer teams. He attends talent shows and other events to support his children. (Tr. pp. 22.) Applicant is and has always been an active member of his church, and his faith is important to him. He has served in various positions of leadership, including a Seminary Teacher and Bishop of his Ward. (Tr. pp. 22-24.)

Policies

When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the adjudicative guidelines (AG). 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 AG ¶ 2 describing the adjudicative process. The administrative judge's overarching adjudicative goal is a fair, impartial, and commonsense decision. According to AG ¶ 2(a), 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." In reaching this decision, I have drawn only those conclusions that are reasonable, logical, and based on the evidence contained in the record.

Directive ¶ E3.1.14, requires the Government to present evidence that establishes 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, and has the ultimate burden of persuasion as to obtaining a favorable clearance decision."

A person who applies for access to classified information seeks to enter 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 protect or safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation as to 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 D, Sexual Behavior

The security concern relating to the guideline for Sexual Behavior is set out in AG ¶ 12:

> 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 standard in this Guideline may be raised solely on the basis of the sexual orientation of the individual.

AG ¶ 13 describes conditions that could raise a security concern and may be disqualifying. The following are potentially applicable:

> (b) 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 guideline at AG ¶ 14 contains conditions that could mitigate security concerns. One is potentially applicable.

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

Applicant viewed pornography on his corporate computer on a number of occasions while at work, and masturbated in the office while at work. He signed a form in 2009 informing him of the Government's concern regarding this misconduct. In 2014, he relapsed and his Special Access was revoked. His behavior over the years has been egregious and inexcusable under any circumstances. Although there is no evidence that he has engaged in this misconduct recently, the behavior continues to casts doubt on his reliability, trustworthiness and judgment. Applicant never contacted his security officer to report his misconduct. If it were not for the polygraph examinations in 2008 and again in 2014, this information may not have been disclosed. Accordingly, this guideline is found against the Applicant.

Guideline M, Use of Information Technology

The security concern relating to the guideline 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:

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

AG ¶ 41 describes conditions that could mitigate security concerns including:

(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.

In addition to engaging in sexual misconduct at work, Applicant loaded unauthorized software onto his corporate computer. Although there is no evidence that he has done this recently, the behavior continues to casts doubt on his reliability, trustworthiness and judgment. Applicant never contacted his security officer to report his misconduct. If it were not for the polygraph examinations in 2008 and 2014, this information may not have been disclosed. Accordingly, this guideline is found against the Applicant.

Guideline E- Personal Conduct

The security concern for Personal Conduct is set out in 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. Of special interest is any failure to cooperate or provide truthful and candid answers during national security investigative or adjudicative processes.

The guideline notes several conditions that could raise security concerns under AG ¶ 16. Two are potentially applicable in this case:

(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:

(2) any disruptive, violent or other inappropriate behavior;

(3) a pattern of dishonesty or rule violations; and

(4) evidence of significant misuse of Government a or other employer's time or resources.

(e) personal conduct, or concealment of information about one's conduct, that creates 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;

There are conditions mitigating security concerns under AG ¶ 17. However, none of them are applicable here:

(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.

Applicant's history of sexual misconduct, misuse of information technology, and poor personal conduct beginning in 2003 and continuing until at least 2014, demonstrates poor judgment, immaturity, and a total disregard for DoD and company policy, regulations, and procedure. This misconduct shows a pattern and gives rise to serious concerns about Applicant's judgment, reliability and trustworthiness, both because of the nature of the offenses, and the circumstances surrounding the offenses. Applicant engaged in this conduct at work, while being entrusted with a security clearance.

It is recognized that Applicant has not engaged in this misconduct for almost ten years, however, given his long history of misconduct, his relapses in sexual misconduct due to his addiction, and the fact that if it were not for the polygraph examinations this information may not have been disclosed, there remains uncertainty and concern about his credibility. The underlying behavior itself is outrageous and egregious, and continues to cast doubt about Applicant's reliability, trustworthiness, and eligibility for access to classified information. Applicant never contacted his security officer to report his misconduct. It was only because of the polygraph examination in 2014, that this

information was disclosed. A decision to determine eligibility for access to classified information will be always be resolved in favor of national security. Under the particular circumstances here, the before-mentioned disqualifying conditions have been established and have not been mitigated.

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 considered the potentially disqualifying and mitigating conditions in light of all facts and circumstances surrounding this case. I have incorporated my comments under Guidelines D, M, and E, in my whole-person analysis. Based upon the facts and analysis set forth above, Applicant has failed to provide sufficient evidence to demonstrate that he meets the qualifications for a security clearance.

Overall, the record evidence leaves me with questions and doubts as to Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude Applicant failed to mitigate the Sexual Behavior, Use of Information Technology, and Personal Conduct security concerns.

Formal Findings

Formal findings for or against Applicant on the allegations set forth in the SOR, as required by ¶ E3.1.25 of the Directive, are:

Paragraph 1, Guideline D:	AGAINST APPLICANT
Subparagraphs 1.a., and 1.b.	Against Applicant.

Paragraph 2, Guideline M: AGAINST APPLICANT

Subparagraphs 2.a., 2.b., and 2.c. Against Applicant.

Paragraph 3, Guideline E: AGAINST APPLICANT

Subparagraphs 3.a., 3.b., and 3.c. Against Applicant

Conclusion

In light of all of the circumstances presented by the record in this case, it is not clearly consistent with the national interest to grant Applicant national security eligibility for a security clearance. Eligibility for access to classified information is denied.

Darlene Lokey Anderson
Administrative Judge