DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 20-02747
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Brian Farrell, Esq., Department Counsel
For Applicant: Carl Anthony Marrone, Esq., Attorney At Law

November 22, 2022

_____

Decision

_____

Lokey Anderson, Darlene D., Administrative Judge:

Statement of the Case

On December 6, 2019, Applicant submitted a security clearance application (e-QIP). (Government Exhibit 4.) On December 13, 2021, the Department of Defense Consolidated Adjudications Facility (DoD CAF) issued Applicant a Statement of Reasons (SOR), detailing security concerns under 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 March 4, 2022, with a written response and attachments A through Y. He requested that his case be decided by an administrative judge on the written record without a hearing. (Item 1.) On June 2, 2022, Department Counsel submitted the Government's written case. A complete copy of the File of

Relevant Material (FORM), containing nine Items, was mailed to Applicant and received by him on June 10, 2022. The FORM notified Applicant that he had an opportunity to file objections and submit material in refutation, extenuation, or mitigation within 30 days of his receipt of the FORM. Applicant submitted his response to the FORM, with a written response and Appendix A through D, which were admitted into evidence. Applicant did not object to Government Items 1 through 9, and they are admitted into evidence, referenced hereinafter as Government Exhibits 1 through 9.

Findings of Fact

Applicant is 29 years old. He is married with no children. He has a Bachelor's degree. He is employed by a defense contractor as an Engineer. He is seeking to obtain a security clearance in connection with his employment.

Guideline M – Use of Information Technology

Prior to his current employment, Applicant worked for another defense contractor from May 2015 to July 2018 at which time, due to his misconduct and violations of company policies, Applicant agreed to resign in lieu of termination. Applicant began working for his current employer in August 2019.

The SOR alleged the following misconduct:

1.a. On multiple occasions between November 2017 and July 2018 Applicant used his company computer (laptop) to stream and view pornographic videos and/or images (sexually explicit material) in violation of company policy. (*See* Applicant's Answer to the SOR.)

1.b. Applicant used the "InPrivate Browsing" mode while using the internet explorer browser to stream and view the explicit pornographic videos and images to evade detection of websites he visited while surfing the internet. The InPrivate Browsing mode allowed him to surf the internet without leaving a digital footprint such as the browsing history, temporary internet files, form data and cookies, which are not retained when the browser is exited. By using this InPrivate Brower mode, Applicant attempted to conceal his behavior knowing it was in violation of company policy.

1.c. Applicant introduced malware computer viruses onto the company's IT System by using his company assigned computer to stream and view pornographic videos and/or images via his YouTube and Instagram accounts. Applicant explained that he realized that he had identified a loophole of sorts where his identity was not associated with his internet browsing. He states that he removed his own access to the resources in a voluntary attempt to end his misconduct on his own, however his misconduct was identified by his employer when he began accessing sexual content through his personal computer's direct network connection and inadvertently introduced malware. He states that it was through the remote server and desktop emulator that he was able to access sexually explicit content at work without discovery dating back to 2017.

Guideline E – Personal Conduct

2.a. See the discussion set forth in subparagraphs 1.a. and 1.c. above.

2.b. In July 2018 Applicant provided false or misleading statements to company officials who were investigating his acts of misconduct described above in subparagraphs 1.a, and 1.c. Applicant changed his response only after being confronted with evidence substantiating his misconduct.

2.c. At the conclusion of the company's investigation, Applicant was given an option to resign in lieu of being terminated form employment for his acts of misconduct described above. Applicant opted to resign. He is not eligible for rehire.

2.d. Applicant provided false or misleading statements to the Department of Defense investigators during his interviews in February and March 2020, by stating that he thought because the site was not blocked, it was acceptable to view content from the site; when in fact he knew viewing explicit content of this sort was not acceptable and that others had gotten into trouble for viewing similar content.

2.e. Applicant completed a security clearance application dated March 29, 2019, and December 6, 2019. In response to Section 13A, which asked him about his "Employment Activities," Applicant provided the reason for leaving his previous employment as there being no long-term career path following an incident involving an inadvertent accessing of malware embedded in a YouTube video while at work. He stated that he had no knowledge that the YouTube video had malware embedded, or that one could embed malware in a YouTube video. Applicant was not truthful in his response. Applicant failed to state the true reason he left. He left in lieu being terminated. Applicant took the option to resign in lieu of being terminated for cause by his company for acts of misconduct described in paragraph 1, above.

2.f. The same questionnaire, also asked Applicant under Section 13A, entitled, "Received Discipline or Warning", about the particulars of the discipline he received. Applicant stated that he was suspended with pay for roughly two weeks for the incident, and that the investigation into the incident with malware was accessed via a YouTube video. Applicant claims that the suspension was with pay, and that it was therefore not considered to be an action of formal discipline by the company. He further stated that he wanted to be honest and forthcoming with his answer. Applicant was not truthful in his response. Applicant's misconduct instigated a formal investigation that concluded that he violated company policy, resulting in his job termination. In lieu of termination, Applicant was suspended without pay during the investigation period, and the company would have fired him for cause had he not taken the option they gave him to resign.

Applicant now acknowledges his sexual addiction, which he believes stems from his childhood trauma of being molested. He admits that he initially attempted to deny his behavior and tried to maintain secrecy until he could no longer keep his problem secret. He admits now that he always knew his actions were wrong, and in violation of company policy. He lied to investigators not only to avoid the consequences of his

actions, but to avoid the shame, pain, and embarrassment of being in front of others and having them know his situation. (Applicant's Response to the FORM.)

He states that he currently attends bi-weekly therapy sessions with his certified sexual addiction therapist/counselor, who helps him to actively pursue health and freedom. He is a member of a sexual addiction support group, is working the program, and is accountable to other group members. After living with his addiction for many years, he believes he has successfully broken the addictive cycle thanks to the help and support of his counselors, support group, and personal support network. He stated that he is committed to ongoing sexual health. (Applicant's Response to the FORM.)

A letter from Applicant's counselor dated February 15, 2022, indicates that Applicant was referred by the pastor of his church for his long-standing pornography addiction. Applicant received a total of eleven sessions of individual or marriage counseling between February 27, 2017, and February 7, 2022, when his attorney requested a summary of the counseling. Applicant is said to have made progress with his addiction before his wife moved out of state. (Applicant's Exhibit D.)

A letter from Applicant's biblical counselor, who provided help to Applicant from 2017 to 2019, indicates that in his opinion, Applicant has stopped engaging in pornography and now realizes the wrong, foolishness, and harm it has caused to his wife and others. Applicant also appears to understand the dangers pornography can have to his personal and professional life. (Applicant's Exhibit E.)

Numerous letters of recommendation from various individuals who know the Applicant well, and some of whom have worked closely with Applicant attest to his exemplary behavior, integrity, reliability and trustworthiness. They all support his request for access to classified information. (Applicant's Exhibits O through X.)

Applicant's performance appraisals for the periods from 2020 and 2021, reflect ratings of "exceeds expectations." (Applicant's Exhibit J.)

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 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;

(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.

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.

None of the mitigating conditions are applicable here. Applicant used his company laptop to view pornography on company property while at work. He knew it was a violation of company policy, and he attempted to conceal his misconduct. He used the InPrivate Browsing Mode to surf the internet to stream and view explicit material without being identified. Applicant also introduced malware viruses onto the company IT system. Although there is no evidence that he has done this recently, the behavior is so egregious, it continues to casts doubt on his reliability, trustworthiness, and judgment. 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. Four are potentially applicable in this case:

(a) deliberate omission, concealment, or falsification of relevant facts from any personnel security questionnaire, personal history statement, or similar form used to conduct investigations, determine employment qualifications, award benefits or status, determine national security eligibility or trustworthiness, or award fiduciary responsibilities;

(b) deliberately providing false or misleading information; or concealing or omitting information, concerning relevant facts to an employer, investigator, security official, competent medical or mental health professional involved in making a recommendation relevant to a national security eligibility determination, or other official government representative;

(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 while-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

(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;

Applicant deliberately lied on his security clearance application in March 2019, in response to questions in Section 13A, about his reasons for leaving his past employment, and whether he received a discipline or warning for misconduct. This misconduct raises the above security concerns.

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.

In response to question 13A, Applicant was not candid or completely truthful in his response to his reason for leaving the job. He stated that there was no long-term path, and that the incident involved an inadvertent accessing of malware embedded in a YouTube video at work. There was no mention of the fact that he was being investigated for violations of company policy, or what the violations entailed, and that in lieu of being terminated, he was given the option to leave or resign.

Furthermore, he was not candid or truthful in response to the question in 13A, concerning his discipline or warning for his misconduct. Applicant stated that he was suspended with pay for two weeks, and that it was not considered to be an action of formal discipline. In the event that Applicant did not consider his discipline to be a formal punitive action, he was wrong. His employer may not have wanted to ruin his career elsewhere, but common sense dictates that if he was no longer qualified to work for his employer, his misconduct was considered very serious. During the investigation, Applicant was suspended without pay, and then he would have been fired for cause, had he not taken the option to resign. There is nothing more punitive than this. Applicant should have been completely truthful in responding to this question.

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 M, and E, in my whole-person analysis. Applicant's misconduct is egregious and unacceptable. Using his company computer to view pornography is in violation of company policy. InPrivate Browsing and any other modes of accessing the internet without leaving a digital footprint is intolerable. Introducing malware to the company IT system is dangerous. In leiu of being terminated from his employment he opted to resign. Furthermore, he has not been truthful or candid with the Government during their investigations and on his security clearance application. 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 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 M:	AGAINST APPLICANT
Subparagraph 1.a.	Against Applicant.
Subparagraph 1.b.	Against Applicant.
Subparagraph 1.c.	Against Applicant.
Paragraph 2, Guideline E:	AGAINST APPLICANT
Subparagraphs 2.a.	Against Applicant
Subparagraphs 2.b.	Against Applicant
Subparagraphs 2.c.	Against Applicant
Subparagraphs 2.d.	Against Applicant
Subparagraphs 2.e.	Against Applicant
Subparagraphs 2.f.	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