DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 23-02407
	)	
Applicant for Security Clearance	)	

Appearances

For Government: John Lynch, Esq., Department Counsel
For Applicant: Daniel P. Meyer, Esq.

01/22/2025

_____

Decision

_____

GOLDSTEIN, Jennifer, Administrative Judge:

Applicant failed to mitigate the security concerns arising under Guidelines D, Sexual Behavior; M, Use of Information Technology; and E, Personal Conduct. National security eligibility for access to classified information is denied.

Statement of the Case

Applicant completed a security clearance application (SCA) on November 3, 2022. On January 12, 2024, the Department of Defense issued to Applicant a Statement of Reasons (SOR) detailing security concerns under the guidelines for Sexual Behavior; Use of Information Technology; and Personal Conduct. Applicant responded to the SOR in an undated submission and requested a hearing before an administrative judge. The case was assigned to me on October 23, 2024.

The hearing was convened as scheduled on December 3, 2024. Government Exhibits (GE) 1 through 6 were admitted in evidence without objection. Applicant testified, and submitted Applicant Exhibits (AE) A through F, which were admitted without

objection. Applicant offered a hearing brief that was marked and received as Hearing Exhibit I. DOHA received the hearing transcript (Tr.) on December 12, 2024.

Findings of Fact

The SOR alleged that Applicant used a government information system between January 2022 and February 2022 to search for sexually explicit material on his social media accounts and to send messages to multiple unidentified females offering them money for sex, under Guidelines M, D, and E. Additionally, under Guideline E, the SOR alleged that in March 2022, he denied the explicit sexual content of the texts and images to government investigators until he was confronted with evidence; that he resigned from his employment after being confronted with his misconduct; and that he falsified his November 23, 2022 SCA, as discussed below. Applicant admitted all SOR allegations. After a thorough review of the testimony, pleadings, and exhibits, I make the following findings of fact:

Applicant is 29 years old and recently married. He obtained a bachelor's degree in 2018. He received a security clearance after graduating college in the summer of 2018. From 2021 to March 2022, Applicant worked as a contractor physical security specialist at a government agency. He received a favorable security clearance adjudication on November 10, 2021, and his eligibility level was SCI. He resigned from that position on March 9, 2022. Since June 2023, he has worked as a senior physical security specialist and antiterrorism officer for another government contractor. (GE 2, GE 3, GE 4; AE C; Tr. 18-21, 48-51)

Applicant used a government computer to access his personal social media accounts on Twitter and Tagged using the unclassified network in a sensitive compartmented information facility (SCIF) at his workplace beginning sometime in December 2021 through early March 2022, with an increasing frequency during that time. He used Twitter to view pornography and Tagged for engaging with women directly via text messages. He sent multiple unidentified females offers to exchange money for sex using his Tagged account. He also received pictures from women showing their genitals through Tagged.

He testified that he was a new employee and thought social media use was permitted on government furnished equipment. He found the rules on social media "vague and confusing." (AE C) He noted that his colleagues used social media to communicate with their spouses. He compared his use of social media to personal communications between spouses. He only used pornographic social media sites while at work because he was afraid his then-girlfriend, now-wife might discover his activities. He said he did not masturbate while viewing the pornography. He indicated that he did not intend to meet the women and pay them for sex, but that he engaged in conversations with them as a "stress reliever." He explained that he was in a troubled mental state at the time due to conflict with his now-wife after her brother was shot and killed by police in October 2020. He felt obligated to take care of the funeral bills and provide financially for her nephew (the deceased brother's son). He looked at pornography because he "was just trying to

find ways to take [his] mind off things and have a bit of stress relief." (Tr. 21-32, 40-42, 48, 58-70, 105-112)

In March 2022, Applicant was confronted by government investigators about his online activity on his government computer. He initially denied that the messages he sent women online were sexual in nature or that the images he viewed depicted sexual interactions. He explained that he "was not truthful in what was going on at the time on my social media accounts because I did not think that's what they were referencing." (Tr. 61-62) He said he was only asked about visiting "porn sites" and that Twitter and Tagged were not specifically porn sites. After he was confronted with details about his online activities including dates and times, he provided the investigators more information about his activities on Twitter and Tagged. The investigators informed him that there was going to be an investigation, and his behavior constituted a security incident. He claimed he was unaware that his job was in jeopardy. At the same time, he claimed he was hearing about a contract change that could also impact his employment. He stated, "Now, they in no way . . . told me that my job was in jeopardy or that, we were going to fire you." (GE 2; Tr. 62) He was told to work from home until the investigation was complete. Applicant submitted his two-week notice that he was resigning from his position with the government contractor within a few days of admitting his sexual misconduct to investigators. He claimed he resigned because the contract was soon to be terminated. (GE 2; AE C; Tr. 61-79)

During his testimony, Applicant acknowledged that his government computer had a notice that appeared during login that warned against viewing pornography. He also admitted to receiving training that employees could not view pornography on a government computer. (Tr. 75-76)

When Applicant completed his SCA on in November 2022, he was asked, in part, if he had been "Fired from a job, Quit a job after being told you would be fired, left a job by mutual agreement following charges or allegations of misconduct . . .?" He failed to disclose that he had resigned from this contractor after being confronted with the misconduct. He answered the question "no." When asked his reason for leaving his employment with the contractor, he answered "Lost Contract" despite knowing that the contract loss was only a rumor at the time and that he resigned after being confronted with his misconduct. He claimed he disclosed the incident during his interviews with Facility Security Officers when applying for jobs, but they said there was nothing in the Defense Information System for Security (DISS) about it. Since it was not reported in DISS, he thought it was resolved. (Tr. 37-38, 99-101)

Applicant also failed to disclose the allegations of computer misuse in his November 2022 SCA when answering Section 27 on his SCA. Section 27 asks, in part, "In the last seven (7) years have you introduced, removed, or used hardware, software, or media in connection with any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines, or regulations or attempted any of the above?" Applicant answered "No" and testified that he deliberately failed to

disclose the allegations on his SCA, because he was "unclear on how to report the situation." (GE 1; Tr. 102-111)

On April 19, 2023, Applicant participated in an enhanced subject interview in response to his SCA. When asked why he resigned his job in March 2022, Applicant answered that it was due to the change in contracting firms. He was then confronted by the interviewer about his misuse of the government computer. Applicant only shared the details of the above events after he was confronted. Applicant then disclosed that he was told during the meeting with investigators "that this violation could potentially affect his job and the [government agency] would be starting an investigation." (GE 2 at 7) On December 16, 2023, Applicant verified the accuracy of this report of the interview. (GE 2) In a March 11, 2024 declaration, Applicant claimed he "made sure to disclose the situation to my background [interviewer] because I wasn't sure how to report the situation properly." (AE C at 2)

Applicant acknowledged at the hearing that his use of the government computer to view pornographic material and offer women money in exchange for sex was "completely wrong." He stated that he now attends therapy monthly. He also completed a pornography screener and sexual addiction questionnaire administered by a licensed clinical social worker, who was not his treating therapist. The screening did not disclose any adverse findings. However, the report from that screening states:

> Patient requested a screener for sexual addictions as required for work. This was our first encounter for 45-60 minutes. It is important to note that his scales came back relatively low. He was counseled on under reporting and risks associated, which he denied . . .[he] explained that he just needed something that said he does not have a sexual addiction. (AE E)

Applicant noted that, through therapy, he learned there are better ways to handle stress like exercise and talking. His family is aware of his misconduct. Since March 2022, he completed annual cyber awareness training in 2022 through 2024 and testified that he has possessed a government phone and laptop without incident. He received a "very rare" spot award from his employer in August 2023. His exhibits highlight several awards and certifications. (GE 2; AE E; Tr. 32-35, 43, 89, 106)

Applicant presented four declarations from personal and professional associates. Applicant's wife wrote that he is trustworthy, dependable, and principled. She indicated she knew of the SOR allegations, but that he was dedicated to personal growth and is deeply passionate about his current work. Three colleagues explained that Applicant is considered both a great coworker and a great friend. He is considered very knowledgeable on the rules and regulations of secured spaces. They all recommend he receive eligibility for a security clearance. (AE D)

Policies

When evaluating an applicant's national security eligibility, the administrative judge must consider the AG. In addition to brief introductory explanations for each guideline, the AG list potentially disqualifying conditions and mitigating conditions, which are 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, these guidelines are applied 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(c), 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. Likewise, I have avoided drawing inferences grounded on mere speculation or conjecture.

Under Directive ¶ E3.1.14, the Government must present evidence to establish controverted facts alleged in the SOR. Directive ¶ E3.1.15 states an "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 seeks access to classified information enters 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 that an applicant may deliberately or inadvertently fail to 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.

Finally, 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.

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

> (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;

Applicant used his government furnished equipment over the unclassified network to view pornography and to solicit sex for money. That constitutes both unauthorized use of the unclassified network and introduction of media prohibited by government policy. Both disqualifying conditions apply.

AG ¶ 41 provides conditions that could mitigate security concerns. I considered all of the mitigating conditions under AG ¶ 41 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;
>
> (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.

Applicant exercised extremely poor judgment in viewing pornography using Twitter and offering women money in exchange for sex over Tagged on his government computer over the unclassified network. His explanation that he was not aware of the rules detract

from his admissions and is hard to believe. He admitted that his logon screen had a notice that pornography was not permitted and that he had received training that included information about the prohibition of pornography. However, he thought he could get around that rule by using his private social media accounts. He also reasoned that it was innocuous conduct. His thought process is concerning. While he has undertaken therapy, has a current reputation for abiding by rules, and is thought to be a knowledgeable security officer, he has not met his burden to show similar misuse of computer conduct is unlikely in the future. His misuse was significant, intentional, and not in the interest of organizational efficiency and effectiveness. None of the above mitigating conditions apply.

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

The guideline notes several conditions that could raise security concerns under AG ¶ 13. The following are potentially applicable in this case:

> (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.

Applicant's solicitation of sex for money at work constitutes behavior that causes vulnerability to coercion and reflects a lack of discretion. His choice to view pornography on his government computer also represents a pattern of high-risk sexual behavior that reflects a lack of discretion or judgment. The evidence is sufficient to raise these disqualifying conditions.

AG ¶ 14 provides conditions that could mitigate security concerns. I considered all of the mitigating conditions under AG ¶ 14 including:

(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; 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.

As noted above, Applicant has not met his burden to show similar conduct is unlikely in the future. AG ¶ 14(b) does not provide mitigation. While he has reduced his vulnerability to coercion, exploitation, or duress by telling his family about the allegations his conduct is not fully mitigated because he has a history of parsing the truth until confronted with the facts about these events. Moreover, he has not been fully forthcoming about these events with the government. AG ¶ 14(c) is not fully applicable.

There is some support for the application of AG ¶ 14(e). Applicant is currently enrolled in therapy and the social worker identified no sexual concerns in the screening he procured. However, his conduct as alleged in the SOR January through February 2022 was serious. He has a history of downplaying his culpability for that conduct. The social worker's questioning of the validity of his low score suggests that not much weight can be afforded to the screening. Further, he provided minimal evidence of treatment. No mitigating condition fully applies.

Guideline E: Personal Conduct

The security concern relating to the guideline 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 following will normally result in an unfavorable national security eligibility determination, security clearance action, or cancellation of further processing for national security eligibility:

(a) refusal, or failure without reasonable cause, to undergo or cooperate with security processing, including but not limited to meeting with a security investigator for subject interview, completing security forms or releases, cooperation with

> medical or psychological evaluation, or polygraph examination, if authorized and required; and
>
> (b) refusal to provide full, frank, and truthful answers to lawful questions of investigators, security officials, or other official representatives in connection with a personnel security or trustworthiness determination.

The guideline at AG ¶ 16 contains seven disqualifying conditions that could raise security concerns. Three disqualifying conditions apply:

> (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; 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 . . .

Applicant falsified his November 2022 SCA in three different places. He answered "no" to the section that asked if he had been left by mutual agreement following charges or allegations of misconduct. In that same section, he was asked his reason for leaving his employment with the contractor, and he answered "Lost Contract" despite knowing that he resigned after being confronted with his misconduct. He also failed to disclose the allegations of computer misuse when answering section 27 on his SCA. AG ¶ 16(a) is applicable.

Applicant also made misleading statements to the government investigator. When he was confronted by government investigators about his online activity using his government computer, he initially denied that the messages he sent women online were sexual in nature or that the images he viewed depicted sexual interactions. AG ¶ 16(b) is applicable.

Applicant's decisions to use a government technology system to search for sexually explicit material and to send messages to women offering money for sex raises independent concerns because it constitutes behavior which, if known, could affect his personal, professional, or community standing. His resignation from his contract

employment after being confronted with his misconduct may also lead to vulnerability. AG ¶ 16(e) is applicable.

The guideline at AG ¶ 17 contains seven conditions that could mitigate security concerns. I considered all of the mitigating conditions including:

> (a) the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts;
>
> (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;
>
> (e) the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress; and
>
> (g) association with persons involved in criminal activities was unwitting, has ceased, or occurs under circumstances that do not cast doubt upon the individual's reliability, trustworthiness, judgment, or willingness to comply with rules and regulations.

Applicant has acknowledged that he should not have searched for sexually explicit material or messaged women with solicitations for sex on his government computer. He has disclosed his conduct to his family, including his wife, who wrote a letter of support. This was a step made to reduce his vulnerability to coercion. He reported that he has not engaged in similar conduct since he resigned from his employment in 2022. He has participated in some therapy. These are factors that support mitigation under AG ¶¶ 17(c), 17(d), 17(e), and 17(g), in part.

In contrast, Applicant has not sufficiently established that he accepts responsibility for his actions and his falsifications. His explanations lack credibility. He likened his use of social media to look at pornography and solicit sex for money to conversations his colleagues had with their spouses. I cannot find that similar conduct is unlikely to occur, given the record evidence. None of the mitigating conditions fully mitigate his false statements or poor judgment.

Whole-Person Concept

Under the whole-person concept, the administrative judge must evaluate an applicant's national security eligibility 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), the ultimate determination of whether to grant national security eligibility 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 pertinent facts and circumstances surrounding this case. The record evidence leaves me with questions and doubts as to Applicant's eligibility and suitability for a security clearance. For all the above reasons, I conclude Applicant failed to mitigate the security concerns arising under Guidelines M, Use of Information Technology; D, Sexual Behavior; and E, Personal Conduct.

Formal Findings

Formal findings for or against Applicant on the allegations set forth in the SOR, as required by ¶ E3.1.25 of Enclosure 3 of the Directive, are:

Paragraph 1, Guideline M:	AGAINST APPLICANT
Subparagraphs 1.a:	Against Applicant
Paragraph 2, Guideline D:	AGAINST APPLICANT
Subparagraphs 2.a:	Against Applicant
Paragraph 3, Guideline E:	AGAINST APPLICANT
Subparagraphs 3.a through 3.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 access to classified information. National security eligibility is denied.

_____
Jennifer I. Goldstein
Administrative Judge