



**DEFENSE LEGAL SERVICES AGENCY
DEFENSE OFFICE OF HEARINGS AND APPEALS**



In the matter of:)
)
) ISCR Case No. 25-01327
)
Applicant for Security Clearance)

Appearances

For Government: Jenny G. Bayer, Esq., Department Counsel
For Applicant: Samir Nakhleh, Esq.

07/31/2026

Decision

HALE, Charles C., Administrative Judge:

Applicant mitigated the concerns raised under the guideline for sexual behavior but did not mitigate the use of information technology and personal conduct security concerns. Eligibility for access to classified information is denied.

Statement of the Case

On December 10, 2025, the Defense Counterintelligence and Security Agency (DCSA) issued a Statement of Reasons (SOR) to Applicant detailing security concerns under Guidelines D (sexual behavior), M (use of information technology), and E (personal conduct). Applicant responded to the SOR on December 17, 2025, and requested a hearing before an administrative judge.

The case was assigned to me on April 7, 2026. The Defense Office of Hearings and Appeals (DOHA) issued a notice of hearing on May 6, 2026, scheduling the hearing for July 15, 2026. The Government requested a continuance, which was granted without objection, and the hearing was convened on July 20, 2026, by mutual agreement of the parties. Government Exhibits (GE) 1 through 5 were admitted in evidence without objection. Applicant testified and submitted Applicant's Exhibits (AE) A through O, which were admitted without objection. Neither party requested that the record remain open. DOHA received the transcript (Tr.) electronically on July 27, 2026.

Findings of Fact

Applicant is a 32-year-old information technology (IT) technician employed by a defense contractor since June 2017. He has worked in the defense industry since about 2015. He is a high school graduate and has taken some college classes. He seeks to retain a security clearance, which he has held since 2014. He has had no security violations prior to this matter. He has various technical certifications in the IT field. He is single and has no children. (Tr. 16-20; GE 1 at 11-12, 32; AE L.)

Applicant denied that while working for a contractor he used his government-issued information technology (IT) at a Government agency “to view inappropriate material and sexually oriented material from about July 13, 2022 until at least January 7, 2023” (SOR ¶¶ 1.a, 2.a, 3.a). In his Answer to the Guideline D allegation, SOR ¶ 1.a, he stated:

I deny this claim. On the weekend of April 1st to April 2nd I thought was a safe site at the time called Yahoo, which, at the time I was using as a news feed. During that time frame, there was a pop up that might have had inappropriate images or videos that came up during that time. Realizing what I did I closed the window that came up. Because it was on Yahoo and that I wasn't on the site for long, I figured I was in the clear, as I remember from my initial security brief at another under the DOD. I am also requesting a copy of the investigation so I can take a look at what they are referring to between Jul. 13, 2022 to Jan. 7, 2023. (Answer at 1.)

SOR ¶ 2.a cross alleged the Guideline D allegation (SOR ¶ 1.a) under Guideline M. In Applicant's Answer to SOR ¶ 2.a he stated:

I admit. I should have reported the information. I figured that I was in the clear due to the brief time it was on the website. Please understand, I did not have our Security Support Office (SSO) phone number or email at the time. Furthermore, I often worked at locations where I was the only person on my team in the room. I couldn't look up the information on Google, and, because it was the weekend, I didn't think a security office was open, not that I knew where it was. I will not make that mistake again. (Answer at 1-2.)

SOR ¶ 3.a cross alleged the Guideline D allegation (SOR ¶ 1.a) under Guideline E. In Applicant's Answer he stated:

I deny this claim. On the weekend of April 1st to April 2nd I thought was a safe site at the time called Yahoo, which, at the time I was using as a news feed. During that time frame, there was a pop up that might have had inappropriate images or videos that came up during that time. Realizing what I did, I closed the window that came up? Because it was on Yahoo and that I wasn't on the site for long, I figured I was in the clear, as I

remember from my initial security brief at another agency under the Department Of Defense.

I admit. I should have reported the information. I figured that I was in the clear due to the short and brief time it was on the website. Please understand, I did not have our Security Support Office (SSO) phone number or email at the time. Furthermore, I often worked at locations where I was the only person on my team in the room. I couldn't look up the information on Google, and, because it was the weekend, I didn't think a security office was open, not that I knew where it was. I will not make that mistake again.

Applicant explained why he was on the yahoo.com website:

So I normally use yahoo.com as one of my news sources. It -- Yahoo can do a lot of things, but it's a news aggregator on one end. So I was looking at stuff like sports, entertainment, world news, U.S. news, stuff like that. (Tr. 24.)

Applicant's conduct was the subject of comprehensive investigation by his agency's Office of the Inspector General (IG). (GE 5.) The IG investigation did a forensic analysis of Applicant's government IT. The investigation recovered 84 universal resource locators (URLs) that contained such words as, "bikini", "topless", "nude", "swimsuit", and "sheer" from his web browser history. The IG investigation concluded the URLs produced "Inappropriate" images to his screen and one URL produced Sexually Oriented Material (SOM). (GE 5 at 10.)

The definitions the IG used for Inappropriate and Sexually Oriented Material were:

Inappropriate: The IG considers inappropriate material as images of men and/or women that are inappropriate for a professional office environment. These images can include, but not limited to, sexually suggestive images of men and/or women with partially exposed breasts, buttocks, and/or genitalia. Inappropriate material does not rise to the level of SOM.

Sexually Oriented Material (SOM): The IG considers SOM as generic nudity/sexual bodily depiction as images and videos of individual human nudity, or groups of nude individuals. Generic nudity/sexual bodily depiction includes, but is not limited to, wearing a covering, sheer or otherwise, that significantly exposes breasts, buttocks, and/or genitalia depicted in circumstances that a reasonable person would determine is sexual in nature. This category also includes sexual contact and/or penetration between individuals or with oneself. Examples of sexual contact include, but should not be limited to, intercourse, masturbation, cunnilingus / fellatio, penetration with objects, or penetration with body parts.

The Government included 30 images that were part of the IG report and were a

portion of the total number of images displayed on Applicant's screen. The images met the IG's definition of "Inappropriate", but it was never established that the images met the generic nudity/sexual body depiction in the SOM definition. There was no evidence in the IG investigation or the record of images of "sexual contact" as set forth in the SOM definition. Neither the IG investigation, nor evidence presented during the hearing indicated which URL triggered the SOM finding. (GE 5 at 7, 9, 10-13, 15-45.)

Applicant did not deny that he had been looking at the articles and images on Yahoo, which he thought was "a safe site" since he was not going into a celebrity's Instagram page. (GE 5 at 10-13; Tr. 54.) He acknowledged the images in the record were on his screen, and that he was typically alone when he was viewing the material. He did not see any need to alter his behavior because these were just news articles from yahoo.com. No evidence was presented of sexual behavior in the workplace. (GE 5 at 15- 45; Tr. 24, 59.) Applicant explained based on his training when the filter was tripped or an alert was sent, he should contact the security office and try to report what exactly happened or what or why it was tripped. (Tr. 71; GE 5 at 15-45.) He explained why he felt it was just a mistake:

This is also the understanding like I said, it's a news aggregator. So Women's Health, would you consider that to be -- I didn't consider that to be -- that's also a professional thing that they had over there, a professional magazine that they have. They had other stuff like, you know, Sports Illustrated. ELLE. ELLE is another one. I figured that those were, you know, professional places. Sure, they have suggestive things, but it wasn't anything that was considered, at least in my understanding, you know, quote, unquote, "porn," I guess. (Tr. 60.)

As the weekend IT person, he had limited work tickets so he had significant down time and while not directly asked, his work environment would not have allowed personal electronic devices. (Tr. 68; Answer.) An employee may use government-provided equipment for personal purposes for limited purposes. The Defense Information System Agency (DISA) Instruction 630-225-15 (DISAI 630-225-15) defines authorized unofficial use as:

5.4 Authorized Unofficial Use. Use of government-provided equipment for personal purposes or communications consistent with the authority document or other DoD issuances. Such use includes personal communications from the employee's usual workplace that are most reasonably made while at the workplace such as, checking in with spouse or minor children; scheduling doctor, automobile, or home repair appointments; brief internet searches; and personal e-mails. Employees may also check their Thrift Savings Plan or other personal investments or seek employment. (GE 5 at 47.)

The DISAI 630-225-15 defines prohibited activities as:

6.2 Government-provided IT and office equipment will not be used for activities prohibited by the authority document, any other DoD issuance, or the unauthorized uses cited in the enclosure. (GE 5 at 47.)

The enclosure to the DISAI 630-225-15 sets forth definitions of unauthorized use of government provided information technology or office equipment. Unauthorized actions were defined as:

To create, download, view, store, copy, or transmit sexually explicit or sexually oriented materials. (GE 5 at 50.)

SOR ¶ 3.b alleged he falsified his answers to Section 13A – Employment Activities:

You falsified material facts on an Electronic Questionnaires for investigations Processing (e-QIP), executed by you on April 30, 2024, when you knowingly and intentionally failed to disclose that, after your employer became aware of the conduct alleged in subparagraph 1.a, you were fired, quit after being told you would be fired, or left after mutual agreement following charges or allegations of misconduct.

Applicant in his Answer denied this allegation stating:

I deny this claim. I think there was confusion as to when I was let go from the organization. Although I was asked to resign due to the information I was given by my company at the time, I was told I was laid off and my position was no longer needed by [Employer]. My company mentioned that it would be written in a way where I wasn't fired and didn't have to write it down as such. Because of this, I didn't think that would apply to the question at the time. I am willing to elaborate further if questioned. (Answer at 2-3.)

Applicant testified he believed he was filling his e-QIP out truthfully. He stated that the company gave him instructions saying, he was not being “fired, necessarily” and that his position was going to be dissolved. He was told not to put down that he was being fired at all and that the company asked him to put in the letter of resignation during that time frame. He was aware he was under investigation, but the company never addressed the matter with him. (Tr. 29, 42-43, 49, 78.)

Applicant's e-QIP listed continuous employment from July 2011 to the date of his March 2024 e-QIP. During this period, he had periods where he was working for multiple employers, and he listed those overlapping periods on his e-QIP. On his resume he also listed continuous employment and including a position that lasted nine months (October 2020 – June 2021), which he annotated with “[temporary position]” and overlapped with a long-term IT position (October 2017 – June 2021). He did not include the IT employment alleged in SOR ¶ 3.b on either his resume or e-QIP. He testified the reason for absence of the IT position in question was because he did not list short-term positions. (GE 1 at 11-21; Tr. 21; AE L.) He stated, “normally when it comes to me not working more than a

year at a job, I normally don't put that on my resume.” He put periods of employment overlap on his resume and e-QIP but not for the period alleged on the SOR. (Tr. 21, 71-77.)

Applicant cited his April 4, 2023 email to his employer where he wrote, “the day has arrived I must put in my resignation due to new opportunities presented to me” for not listing being fired. He acknowledged he knew he was under investigation at the time of the email. (AE M; Tr. 47-50, 78.) Applicant’s 2024 e-QIP (GE 1) asked two questions in succession as part of the query for a period of employment:

For this employment have any of the following happened to you in the last seven (7) years?

- Fired
 - Quit after being told you would be fired
 - Left by mutual agreement following charges or allegations of misconduct
 - Left by mutual agreement following notice of unsatisfactory performance
- Yes: { } . No: { } .

Summary of Reasons for Leaving

For this employment, in the last seven (7) years have you received a written warning, been officially reprimanded, suspended, or disciplined for misconduct in the workplace, such as a violation of security policy?

Yes: { } . No: { } .

For the first question, Applicant never marked having any of the listed events as a cause for him leaving employment. However, in the next question, Applicant twice marked “Yes” for receiving a written warning, after which he gave a brief summary of the reason for both occasions, a 2018 incident over a work refusal and a 2017 incident over a timecard issue. (GE 1 at 16, 18; Tr. 72, 77.) He could not address why he marked yes and elaborated on being reprimanded in 2017 and 2018 but provided nothing on his e-QIP about his resignation or that he had ever been employed by the company. (Tr. 77-78.)

Applicant’s testimony that he did not deliberately falsify his e-QIP was not credible. He omitted the entire employment period from his e-QIP and resume. He was aware of the investigation when he resigned. He was an IT technician, and he knew viewing the material in question on his agency’s computer at his worksite was prohibited but figured that he “was in the clear due to the short and brief time” he was on the websites. (Answer; Tr. 21, 78.)

Policies

This case is adjudicated 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), which became effective on June 8, 2017.

When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the adjudicative guidelines. 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 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."

Under Directive ¶ E3.1.14, the Government must present evidence to establish 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." The applicant has the ultimate burden of persuasion to obtain a favorable security 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 the applicant may deliberately or inadvertently fail to safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation of 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 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.

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

- (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 and/or that reflects lack of discretion or judgment.

Applicant refuted the sexual behavior allegation. He actions occurred on the Yahoo website searching for known celebrities, which did not establish a pattern of compulsive, self-destructive, or high-risk sexual behavior that he was unable to stop. No evidence was provided that he engaged in sexual behavior in the workplace. The above disqualifying conditions have been refuted.

Guideline M, Use of Information Technology

The security concern 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 is potentially applicable:

(e) unauthorized use of any information technology system.

Applicant knew he was violating IT policy when he accessed “Inappropriate” and “Sexually Oriented Material” on his Agency’s IT system, while working as the weekend IT helpdesk technician. The above disqualifying condition is applicable.

Conditions that could mitigate the use of information technology systems security concerns are provided under AG ¶ 41. The following is potentially applicable:

(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; and

(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.

Applicant’s inappropriate conduct is recent, and he did not acknowledge its inappropriateness until he received the SOR. The evidence shows he was viewing material on the Yahoo website which could potentially fall into the authorized unofficial use definition. There was no evidence he was seeking pornography. The material he viewed did not trigger him to see a requirement for reporting an unintentional or inadvertent situation requiring a prompt, good faith effort to correct the situation and a notification to appropriate personnel. However, he left this period of employment off both his resume and e-QIP, which cast doubt on his willingness to correct the situation and provide notification to appropriate personnel. Given his search terms, this was not unintentional or inadvertent conduct, nor consistent with brief authorized internet searches. When he got into areas he recognized were inappropriate, he admitted he did not make a prompt, good faith effort to correct the situation by notification to appropriate personnel. Leaving the period of employment in question off both his resume and e-QIP, cast doubt on his current reliability, trustworthiness, or good judgment and willingness to correct the situation and provide notification to appropriate personnel. His conduct continues to cast doubt on his reliability, trustworthiness, and good judgment. Neither AG ¶¶ 41(a) or 41(c) are applicable.

Guideline E, Personal Conduct

The security concern for personal conduct is set out in AG ¶ 15, as follows:

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 clearance investigative or adjudicative processes.

AG ¶ 16 describes conditions that could raise a security concern and may be disqualifying. The following disqualifying conditions are potentially applicable:

(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;

(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; 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.

AG ¶¶ 16(a) 16(b) 16(c) and 16(e) are applicable. Applicant willfully did not disclose conduct at work that caused his resignation on his e-QIP, the misuse of his government computer, because he knew that it would be problematic for his security clearance. His explanation that he resigned to pursue other opportunities was not credible.

AG ¶ 17 provides conditions that could mitigate security concerns. The following are potentially applicable:

(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; and

(e) the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress.

SOR ¶¶ 3.a and 3.b, Applicant denied his misuse of information technology, which he did not include in the relevant section of his e-QIP. He continued to blame the Yahoo search engine for allowing him to view inappropriate URLs but did not accept full responsibility for using search terms like “bikini”, “topless”, “nude”, “swimsuit”, and “sheer”. The above analysis under misuse of information technology also applies here to his personal conduct.

None of the mitigating conditions are applicable. Applicant's conduct is recent. He was not credible when he said he had not deliberately provided false information on his e-QIP. The omission on his e-QIP and then his omission on his personal resume demonstrates his intent to conceal his conduct, which cast doubt on his reliability, trustworthiness, and good judgment. His active concealment of his conduct is a negative step which makes him vulnerable to exploitation, manipulation, and duress. AG ¶¶ 17(a), 17(c), and 17(e) and do not apply.

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 the facts and circumstances surrounding this case. I considered that Applicant's 10-year history of maintaining a security clearance without any security issues. However, an applicant's prior good security record is not a bar to an unfavorable adjudication, and the Government “need not

wait until an individual mishandles or fails to safeguard classified information before it can make an unfavorable security clearance decision.” See ISCR Case No. 08-00435, 2009 WL 848722 at *2 (App. Bd. Jan. 22, 2009) *citing* Adams v. Laird, 420 F.2d 230, 238-39 (D.C. Cir. 1969). I have incorporated my comments under Guidelines D, M, and E in my whole-person analysis.

Overall, the record evidence leaves me with questions and doubts about Applicant’s eligibility and suitability for a security clearance. I conclude Applicant did mitigate the sexual behavior concern but did not mitigate use of information technology or personal conduct security concerns.

Formal Findings

I make the following formal findings on the allegations in the SOR:

Paragraph 1, Guideline D:	FOR APPLICANT
Subparagraph 1.a:	For Applicant
Paragraph 2, Guideline M:	AGAINST APPLICANT
Subparagraph 2.a:	Against Applicant
Paragraph 3, Guideline E:	AGAINST APPLICANT
Subparagraphs 3.a-3.b:	Against Applicant

Conclusion

It is not clearly consistent with the national interest to grant Applicant eligibility for a security clearance. Eligibility for access to classified information is denied.

Charles C. Hale
Administrative Judge