



**DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS**



In the matter of:)	
)	
[Redacted])	ISCR Case No. 22-01200
)	
Applicant for Security Clearance)	

Appearances

For Government: William H. Miller, Esq., Department Counsel
For Applicant: *Pro se*

03/27/2025

Decision

FOREMAN, LeRoy F., Administrative Judge:

This case involves security concerns raised under Guidelines D (Sexual Behavior), E (Personal Conduct), J (Criminal Conduct), and M (Use of Information Technology). Clearance is denied.

Statement of the Case

Applicant submitted a security clearance application (SCA) on August 25, 2020. On May 10, 2023, the Defense Counterintelligence and Security Agency (DCSA) sent him a Statement of Reasons (SOR) alleging security concerns under Guidelines D, E, J, and M. The DCSA acted under Executive Order (Exec. Or.) 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; Department of Defense (DOD) Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the adjudicative guidelines (AG) promulgated in Security Executive Agent Directive 4, *National Security Adjudicative Guidelines* (December 10, 2016), which became effective on June 8, 2017.

Applicant answered the SOR on June 7, 2023, and denied all the allegations. Department Counsel was ready to proceed on June 28, 2024, and the case was assigned to me on January 8, 2025. On January 15, 2025, the Defense Office of Hearings and Appeals notified Applicant that the hearing was scheduled to be conducted on February 11, 2025. I convened the hearing as scheduled. Government Exhibits 1 through 4 were admitted in evidence without objection.

Applicant testified and submitted Applicant's Exhibits (AX) 1 through 21. AX 1 through 16 and 18 through 21 were admitted without objection. AX 17, discussed below, was not admitted. DOHA received the transcript on February 24, 2025.

Evidentiary Issue

Before the hearing convened, Applicant proffered AX 17, a polygraph examiner's report expressing an opinion about Applicant's veracity. Department Counsel filed a motion *in limine* to exclude this evidence. (Hearing Exhibit I) I sustained Department Counsel's objection, on the ground that the results of a polygraph regarding the truthfulness of the statements made during the examination are not admissible. See ISCR Case No. 02-31428 at 4 (App. Bd. Jan. 20, 2006).

Jurisdiction

In Applicant's answer to the SOR, he stated that his employer "will withdraw my clearance request based on my job not requiring the top-secret clearance." This statement was incorrect. The Defense Information System for Security (DISS) reflected that he was sponsored for a clearance by his current employer at the time the hearing commenced. The documentation establishing jurisdiction is attached to the record as Hearing Exhibit II.

Findings of Fact

Applicant is a 67-year-old consulting chief engineer employed by a defense contractor since August 2005. He holds multiple master's degrees, including a master's degree in computer systems management in December 1992, a master's degree in telecommunication management in May 2010, a master's degree in cyber security in December 2013, and a master's degree in business administration in May 2017. He received a doctorate in church consulting in 2011, and he has served as a deacon in his church for 16 years. (AX 20 at 3) He married in September 1986. He has two adult daughters and an adult son. He received a security clearance in April 1997 and received eligibility for access to sensitive compartmented information (SCI) in April 2011. His SCI eligibility was revoked in March 2012, and his eligibility for access to classified information was revoked on a date not reflected in the record.

Under Guideline D, the SOR alleges that Applicant viewed child pornography from about 1988 to 2011 (SOR ¶ 1.a), that he used his company-issued computer to view child pornography on multiple occasions (SOR ¶ 1.b), and that he used his company-issued computer to view other pornography on multiple occasions (SOR ¶ 1.c).

Under Guideline E, SOR ¶ 2.a alleges that Applicant falsified material facts during a personal subject interview (PSI) in July 2017 by stating that his clearance was denied due to a polygraph officer misinterpreting the answers he provided to routine questions when in fact he deliberately sought to conceal the information alleged in SOR ¶¶ 1.a through 1.c. It also alleges in SOR ¶ 2.b that, during the October 2011 PSI, he deliberately falsified material facts and concealed the information set forth in SOR ¶¶ 1.a through 1.c. SOR ¶ 2.c cross-alleges the conduct in SOR ¶¶ 1.a through 1.c under this guideline. Under Guideline J, SOR ¶ 3.a cross-alleges the conduct alleged in SOR ¶¶ 1.a and 1.b. Under Guideline M, SOR ¶ 4.a alleges that Applicant manipulated software without authorization when he intentionally circumvented firewall and content filters while working, in order to view pornography.

When Applicant applied for SCI eligibility, he underwent a counterintelligence polygraph examination, and no security concerns arose during that examination. He was scheduled for a lifestyle examination in May 2011. According to the polygraph examiner's report, Applicant disclosed during a pretest discussion that he had accidentally viewed adult pornography while at work and searching for movie and celebrity information. In a post-test discussion, he explained that he used the search terms "Asian woman" and "Asian movie star." These neutral terms were not likely to be blocked by the company's firewalls. He admitted that, when he clicked on this site, he briefly viewed thumbnails of fully clothed Asian women and some naked women. (GX 2 at 56) He admitted viewing about 200 images while at work. (GX 2 at 9)

At the hearing, Applicant testified that he viewed the website, "Happy Asian Women," during his lunch time, and it did not include any pornography. He testified that his employer had a firewall infrastructure that monitored and recorded every site that he visited. He admitted at the hearing that he searched for "Asian Women" or "Asian Movie Stars," but he denied searching for pornography. (Tr. 44-45) He denied telling the polygraph examiner that he viewed pornography at work, but he admitted telling the polygraph examiner that he viewed pornography at home on his personal computer. (Tr. 47-48) He denied telling the polygraph examiner that the filters on his work computer were set at the lowest level. He explained that only a company administrator could control the content filters. (Tr. 49) He submitted documentary evidence showing how firewalls work. (AX 14) He admitted telling the polygraph examiner that he opened a webpage that contained images of girls who appeared to be 12 or 13 years old, but that he immediately closed it and did not download any images or content. (Tr. 50)

The polygrapher's report on the pretest and post-polygraph examination recites that all the information was reviewed with Applicant and he concurred in its accuracy. (GX 2 at 17) At the hearing, Applicant testified that he never had a chance to review the accuracy of the report. (Tr. 58)

Applicant underwent another polygraph examination on September 13, 2011. According to the polygraph examiner's report, he stated that he searched for images on Google, using terms such as "teenage girls" or "Lolita," but that he never deliberately viewed images of anyone he thought was under 18 years old. (GX 2 at 10) At the hearing, he testified that he did not give the polygraph examiner specific search terms such as

“teenage girls” or “Lolita,” but he gave him the name of another pornography website. (Tr. 53)

Applicant underwent another polygraph examination in October 2011. During the pretest interview, he denied intentionally seeking pornography involving anyone under the age of 18. He also denied viewing any website that did not include a legal disclaimer stating that all the persons portrayed are 18 years old or older. In the post-test interview, he stated that he had accidentally opened files containing images of females between 13 and 15 years old. At the hearing, he admitted telling the polygraph examiner that he accidentally opened these files, and he admitted telling the polygraph examiner that he was concerned about impact of this event on his security clearance and his job. (GX 2 at 10-11)

Applicant underwent another polygraph examination in November 2011. During the pretest interview, he admitted that he sought out, viewed, became aroused, and masturbated to child pornography about once a month from 1988 until he was interviewed in September 2011. (GX 2 at 11)

Applicant applied for reinstatement of his clearance in the spring of 2016. In July 2017, Applicant was interviewed about his prior clearances, and he told the investigator that he previous application for a clearance was denied because the polygraph examiner misinterpreted his answers to routine questions during the polygraph examination. (GX 2 at 12) He told the investigator that he did not know what was misinterpreted because he was not able to see the polygraph examiner’s report. (GX 3 at 12)

At the hearing, Applicant testified that he has not viewed any child pornography, either at work or at home, since 2011. (Tr. 63) In a sworn declaration submitted at the hearing, he stated:

As a Christian . . . I have struggled with porn based on my faith, but I believe as a mature adult, watching pornographic material was acceptable behavior within my private space at home. Since my clearance revocation in March [2011], I have not seen any pornographic materials, and will not view any pornographic materials in the rest of my life. . . .

I never thought that my actions of watching pornographic material could result in this revocation. . . . In a way, it has helped me to look back and see how numb my moral senses were while watching the adult pornographic materials. I am truly sorry that the adult video contains real people and they might have been models under 18 years old despite the fact that there was no way to [be] certain of their ages.

(AX 20 at 5-8)

There is no evidence that Applicant has attempted to view pornography on his company-issued computer at work since March 2011. He presented no evidence corroborating his claim that he has not viewed pornography at home since March 2011.

Numerous supervisors and coworkers submitted letters supporting Applicant's appeal of his security clearance in 2011. They reflect that he was highly regarded for his technical skills, judgment, integrity, and trustworthiness. (AX 1-11, 15, 18, 19) He resubmitted them at the hearing, and I have considered them.

Policies

"[N]o one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988). As Commander in Chief, the President has the authority to "control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to have access to such information." *Id.* at 527. The President has authorized the Secretary of Defense or his designee to grant applicants eligibility for access to classified information "only upon a finding that it is clearly consistent with the national interest to do so." Exec. Or. 10865 § 2.

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

The Government reposes a high degree of trust and confidence in persons with access to classified information. This relationship transcends normal duty hours and endures throughout off-duty hours. Decisions include, by necessity, consideration of the possible risk that the applicant may deliberately or inadvertently fail to safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation about potential, rather than actual, risk of compromise of classified information.

Clearance decisions must be made "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." Exec. Or. 10865 § 7. Thus, a decision to deny a security clearance is merely an indication the applicant has not met the strict guidelines the President and the Secretary of Defense have established for issuing a clearance.

Initially, the Government must establish, by substantial evidence, conditions in the personal or professional history of the applicant that may disqualify the applicant from being eligible for access to classified information. The Government has the burden of establishing controverted facts alleged in the SOR. *See Egan* at 531. Substantial evidence is "such relevant evidence as a reasonable mind might accept as adequate to support a conclusion in light of all the contrary evidence in the same record." *See* ISCR Case No. 17-04166 at 3 (App. Bd. Mar. 21, 2019) It is "less than the weight of the evidence, and the possibility of drawing two inconsistent conclusions from the evidence does not prevent [a Judge's] finding from being supported by substantial evidence." *Consolo v. Federal Maritime Comm'n*, 383 U.S. 607, 620 (1966). "Substantial evidence" is "more than a scintilla but less than a preponderance." *See v. Washington Metro. Area*

Transit Auth., 36 F.3d 375, 380 (4th Cir. 1994). The guidelines presume a nexus or rational connection between proven conduct under any of the criteria listed therein and an applicant's security suitability. ISCR Case No. 15-01253 at 3 (App. Bd. Apr. 20, 2016).

Once the Government establishes a disqualifying condition by substantial evidence, the burden shifts to the applicant to rebut, explain, extenuate, or mitigate the facts. Directive ¶ E3.1.15. An applicant has the burden of proving a mitigating condition, and the burden of disproving it never shifts to the Government. See ISCR Case No. 02-31154 at 5 (App. Bd. Sep. 22, 2005).

An applicant "has the ultimate burden of demonstrating that it is clearly consistent with the national interest to grant or continue his security clearance." ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002). "[S]ecurity clearance determinations should err, if they must, on the side of denials." *Egan* at 531.

Analysis

Guideline D, Sexual Behavior

The allegations under this guideline are overlapping. When the same conduct is alleged more than once in the SOR under the same guideline, one of the duplicative allegations should be resolved in Applicant's favor. ISCR Case No. 03-04704 at 3 (App. Bd. Sep. 21, 2005). SOR ¶¶ 1.a and 1.b both allege viewing of child pornography, with SOR ¶ 1.a alleging a specific time period (1988 to September 2011) and SOR ¶¶ 1.b not alleging a time period. SOR ¶¶ 1.b and 1.c both allege viewing pornography on a company-issued computer. I have resolved SOR ¶ 1.b in Applicant's favor because it overlaps both SOR ¶¶ 1.a and 1.c.

The concern under this guideline 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. . . .

The following disqualifying conditions under this guideline are relevant:

AG ¶ 13(a): sexual behavior of a criminal nature, whether or not the individual has been prosecuted;

AG ¶ 13(b): pattern of compulsive, self-destructive, or high-risk sexual behavior that the individual is unable to stop; and

AG ¶ 13(c): sexual behavior that causes an individual to be vulnerable to coercion, exploitation, or duress.

All three disqualifying conditions are established. Applicant has admitted that he struggles with pornography because of his Christian faith. Although he has claimed that the polygraph examiners misinterpreted his statements during the pretest interviews and post-hearing discussions, he was unable to identify what comments they might have misinterpreted. It is not likely that three separate polygraph examiners would have misinterpreted his comments.

Conditions that could mitigate security concerns under this guideline include:

AG ¶ 14(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

AG ¶ 14(c): the behavior no longer serves as a basis for coercion, exploitation, or duress.

AG ¶ 14(b) is not established. Applicant has asserted that he has not viewed any pornography at home or at work since his clearance was revoked in 2011. There is no evidence that contradicts his assertion and no evidence that corroborates it. However, he has a history of conflicting admissions, denials, and recantations that raise doubt about his credibility. In October 2011, he told an investigator that he opened files containing child pornography by accident. In November 2011, he told an investigator that his October 2011 statement was false. At the hearing, he recanted his November 2011 admission that his October 2011 statement was false. Applicant has the burden of establishing mitigating circumstances. He has not carried that burden with respect to AG ¶ 14)(b).

AG ¶ 14(c) is not established. Applicant's history of viewing of child pornography continues to humiliate and embarrass him and make him vulnerable to coercion, exploitation, or duress.

Guideline E, Personal Conduct

The security concern under this guideline 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 disqualifying conditions under this guideline are relevant:

AG ¶ 16(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

AG ¶ 16(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 . . . :engaging in activities which, if known, could affect the person's personal, professional, or community standing.

AG ¶ 16(b) is established. During the post-test interview in October 2011, Applicant falsely told the polygraph examiner that he opened files containing images of females between 13 and 15 years old by accident. During the July 2017 PSI, he falsely told the investigator that his previous application for a clearance was denied because a polygraph examiner misinterpreted his answers during the polygraph examination.

The following mitigation conditions are relevant:

AG ¶ 17(a): the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts;

AG ¶ 17(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;

AG ¶ 17(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

AG ¶ 17(e): the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress;

AG ¶ 17(a) is not established. During a pretrial interview with another polygraph examiner in November 2011, he admitted that his October 2011 statement was false, that his viewing of child pornography was not accidental, and that he intentionally sought out, viewed, became aroused, and masturbated to child pornography about once a month from 1988 until he was interviewed in September 2011. However, at the hearing, he recanted his admission during the November 2011 interview that his October 2011 statement was false. (Tr. 57) He continues to maintain that the allegations against him are based on a polygraph examiner's misinterpretation of his answers to questioning.

AG ¶ 17(c) is not established. Applicant's false statement in October 2011 and July 2017 were not "minor." Falsification during a security interview undermines the integrity of the security clearance process.

AG ¶ 17(d) is not fully established. Applicant submitted no evidence of counseling or other steps to alleviate the stressors, circumstances, or factors that contributed to his involvement with pornography.

AG ¶ 17(e) is not fully established. Applicant has declared his intention to refrain from viewing any child pornography. However, he remains vulnerable to influence or coercion because of his past involvement in child pornography.

Guideline J, Criminal Conduct

The concern under this guideline is set out in AG ¶ 30: “Criminal activity creates doubt about a person's judgment, reliability, and trustworthiness. By its very nature, it calls into question a person's ability or willingness to comply with laws, rules, and regulations.”

The relevant disqualifying condition is AG ¶ 31(b): “evidence (including, but not limited to, a credible allegation, an admission, and matters of official record) of criminal conduct, regardless of whether the individual was formally charged, prosecuted, or convicted.” Applicant admits that viewing child pornography is illegal and he admitted in the November 2011 pretest interview with a polygraph examiner that he sought out and viewed child pornography from 1988 until he was interviewed in September 2011.

The following mitigating conditions are potentially applicable

AG ¶ 32(a): so much time has elapsed since the criminal 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

AG ¶ 32(d): there is evidence of successful rehabilitation; including, but not limited to, the passage of time without recurrence of criminal activity, restitution, compliance with the terms of parole or probation, job training or higher education, good employment record, or constructive community involvement.

Neither mitigating condition is established. Significant time has elapsed since Applicant's falsification in October 2011. In November 2011, he corrected his falsifications, but at the hearing, he recanted his November 2011 statement. He has not accepted responsibility for his falsifications during the security-clearance process. When an applicant is unwilling or unable to accept responsibility for his or her own actions, such a failure is evidence that detracts from a finding of reform and rehabilitation. See ISCR Case No. 17-01680 (Jul. 19, 2019).

Guideline M, Misuse of Information Technology

The concern under this Guideline 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 following disqualifying conditions under this guideline are potentially applicable:

AG ¶ 40(b): unauthorized modification, destruction, or manipulation of, or denial of access to, an information technology system or any data in such a system; and

AG ¶ 40(e): unauthorized use of any information technology system.

Both disqualifying conditions are established. Applicant submitted information showing how firewalls prevent downloading or viewing prohibited materials. He did not modify or destroy any firewalls or filters. Instead, he deliberately circumvented the system by using benign key words ("Asian woman" or "Asian movie star") in his searches that would not trigger the protective firewalls or filters.

The relevant mitigating condition is AG ¶ 41(a):

[S]o 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.

This mitigating condition is established. Applicant last viewed pornography on his company-issued computer in September 2011. The revocation of his security clearance, his personal embarrassment, and his fear of losing his job makes his misuse of a company-issued computer unlikely to recur.

Whole-Person Analysis

Under AG ¶ 2(c), the ultimate determination of whether to grant a security clearance must be an overall commonsense judgment based upon careful consideration of the guidelines and the whole-person concept. An administrative judge must evaluate an appellant's security eligibility by considering the totality of the appellant's conduct and all the relevant circumstances. An 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.

I have incorporated my comments under Guidelines D, E, J, and M in my whole-person analysis and applied the adjudicative factors in AG ¶ 2(d). After weighing the disqualifying and mitigating conditions under those guidelines and evaluating all the evidence in the context of the whole person, I conclude Applicant has mitigated the security concerns raised under Guideline M, but he has not mitigated the security concerns raised under Guidelines D, E, and J.

Formal Findings

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

Paragraph 1, Guideline D, Sexual Behavior:	AGAINST APPLICANT
Subparagraph 1.a:	Against Applicant
Subparagraph 1.b:	For Applicant
Subparagraph 1.c:	Against Applicant
Paragraph 2, Guideline E, Personal Conduct:	AGAINST APPLICANT
Subparagraphs 2.a-2.c:	Against Applicant
Paragraph 3, Guideline J, Criminal Conduct:	AGAINST APPLICANT
Subparagraph 3.a	Against Applicant
Paragraph 4, Guideline M: Misuse of IT:	FOR APPLICANT
Subparagraph 4.a:	For Applicant

Conclusion

I conclude that it is not clearly consistent with the national security interests of the United States to grant Applicant eligibility for access to classified information. Clearance is denied.

LeRoy F. Foreman
Administrative Judge