



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



In the matter of:)
)
) ISCR Case No. 19-03536
)
Applicant for Security Clearance)

Appearances

For Government: Jeff Nagel, Esq., Department Counsel
For Applicant: Jeffrey S. Gard, Esq.

02/25/2022

Decision

COACHER, Robert E., Administrative Judge:

Applicant failed to mitigate the Government’s security concerns under Guideline D, sexual behavior, Guideline M, use of information technology, and Guideline E, personal conduct. Applicant’s eligibility for a security clearance is denied.

Statement of the Case

On October 23, 2020, the Department of Defense (DOD) issued Applicant a Statement of Reasons (SOR) detailing security concerns under Guideline D, sexual behavior, Guideline M, use of information technology, and Guideline E, personal conduct. The DOD acted 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) implemented by the DOD on June 8, 2017.

Applicant answered the SOR on December 3, 2020, and requested a hearing. The case was assigned to me on October 21, 2021. The Defense Office of Hearings and Appeals (DOHA) issued a notice of hearing on November 3, 2021, and the hearing was held as scheduled on November 17, 2021. (Applicant's counsel agreed to the November 17, 2021 hearing date on October, 27, 2021, See Hearing Exhibit (HE) II) The Government offered exhibits (GE) 1 through 8, which were admitted into evidence without objection. The Government's exhibit list was marked as HE I. Applicant testified and offered exhibits (AE) A and B, which were admitted into evidence without objection. The record was held open until November 30, 2021, to allow Applicant to provide additional evidence. He timely submitted AE C, which was admitted without objection. DOHA received the hearing transcript (Tr.) on November 29, 2021.

Findings of Fact

In Applicant's Answer, he admitted all the SOR allegations, with explanations. The admissions are adopted as findings of fact. After a thorough and careful review of the pleadings and evidence submitted, I make the following additional findings of fact.

Applicant is 68 years old. He is married (his third marriage) and has no children of his own. He currently works for a defense contractor for whom he has worked for approximately six years. He has a bachelor's degree. He first received a security clearance sometime in the 1980s. In 2016, his active security clearance was suspended by the Defense Security Service (DSS) for the allegations at issue in this hearing. His current employer is sponsoring him for his security clearance request. (Tr. 20, 37-38; GE 1, 5)

Under Guideline D, the SOR alleged the following: (1) that Applicant, between 2001 and 2015, used his company-issued computer to upload, view, and save images of naked women and young girls, ages 11-15, in modeling poses and with scant clothing. It also alleged Applicant continues to view similar images at home on his cell phone; (2) that in January 1997, Applicant was arrested and charged with sexual assault and sexual assault on a child while in a position of trust; and (3) that Applicant attended a 12-step program for sex addicts from 2001 to 2016, but stopped attending because his wife did not think it was helping him. (SOR ¶¶ 1.a-1.c) I find that SOR ¶ 1.c does not fall within any of Guideline D's disqualifying conditions and further find for the Applicant on this allegation.

Under Guideline M, the SOR alleged the following: (1) that Applicant signed documents prepared by his employer, for whom he worked from 2001 to 2015, that prohibited him from using his company-issued computer to view any pornography; and (2) that Applicant, between 2001 and 2015, used his company-issued computer to upload, view, and save images of naked women and young girls, ages 11-15, in modeling poses and with scant clothing. It also alleged Applicant continues to view similar images at home on his cell phone. (SOR ¶¶ 2.a-2.b)

Under Guideline E, the SOR alleged: (1) that in February 2015, Applicant was removed from his work premises, had his work laptop and security badges confiscated for violations of personal conduct and violations of his company's network information technology systems; (2) that in March 2015, Applicant was terminated from his employment; (3) that Applicant, between 2001 and 2015, used his company-issued computer to upload, view, and save images of naked women and young girls, ages 11-15, in modeling poses and with scant clothing. It also alleged Applicant continues to view similar images at home on his cell phone; and (4) that Applicant signed documents prepared by his employer, whom he worked for from 2001 to 2015, that prohibited him from using his company-issued computer to view any pornography. (SOR ¶¶ 3.a-3.c)

In approximately 1997, Applicant was arrested for inappropriately touching his 11-year-old stepdaughter. He touched her through her clothing when she was sleeping (or pretending to sleep). He did this once a week for a month. The child told her mother (Applicant's second wife) about Applicant's actions. He admitted his behavior. He also admitted viewing images of adolescent girls ages 11 to 15 in sexually erotic poses during this time. He was arrested on felony charges of sexual assault on a child and sexual assault on a child while in a position of trust. He pleaded guilty and was given a deferred sentence, which included four years of unsupervised probation. He was also ordered to attend treatment by a therapist for four years. He was ordered to register as a sex offender. He successfully completed his probation, including attending his court-ordered treatment. He was released from probation and successfully fulfilled the terms of his deferred sentence in 2001. The original charges were then dropped. From 2001 to 2016, he voluntarily attended a 12-step recovery program for sex addicts. He believed the meetings were helpful, but his wife did not, so he stopped attending. He is no longer listed as a sex offender in his home state. In his SOR answer, Applicant claimed that a therapist gave him a favorable prognosis against reoffending. He did not offer any records to document of said prognosis or discuss his treatment history. (Tr. 27, 37-38, 40; GE 2, 7; AE C; SOR answer)

From June 2001 to March 2015, Applicant worked for employer 1 (E1) as a software engineer. In his interview with a defense investigator in July 2019, Applicant admitted that he signed documents provided by E1, or E1's predecessor company, acknowledging that he was prohibited from having and viewing pornography on his company-provided computer. In his hearing testimony, Applicant equivocated this point stating that he could not recall any specific formal company policy regarding the personal use of a company-issued laptop. He also stated that someone told him he could use his company-issued laptop for personal use, but he could not recall who that person was. I did not find Applicant's testimony credible. (Tr. 23, 30, 34; GE 2; SOR answer)

In February 2015, law enforcement became aware that Applicant may have had child pornography on his company-issued laptop. In October 2015, Applicant's work laptop was seized and examined by law enforcement forensic examiners. The examination concluded that the material found on the computer was not child pornography, but rather child erotica (adolescent children posed in erotic positions with

skimpy and/or revealing clothing). Possessing child erotica on a computer does not violate any state law where Applicant was located. The criminal investigation was closed. Applicant admitted have adult pornography on his employer-provided laptop. (Tr. 28; GE 2, 8)

In February 2015, Applicant's employer put him on administrative leave pending the criminal investigation into his alleged computer misuse. In March 2015, due to the uncertainty of his computer activities, his employment was terminated with E1 and he was directed to return all the government and E1 property issued to him. In April 2016, he received notification from the DSS that his security clearance was suspended based on information obtained by DOD regarding his sexual behavior and criminal conduct. In his SOR answer, he admitted using his company-issued laptop to view, upload, and save images of naked women and scantily dressed young girls (ages 11-15) posed in erotic positions. He also admitted signing company documents prohibiting him from using his company-laptop for these purposes. (Tr. 23-24, 28-29, 34-35; GE 2, 4, 5; SOR answer)

Applicant denied using his current company-issued computer to view, download, or save any type of pornographic material. He documented that he has no criminal record in his home state, other than the 1997 child sexual abuse crime. He admitted that he continues to view child erotica on his personal electronic devices. He viewed these types of images as recently as a month before his security clearance hearing. He continues to view this material because he is sexually stimulated by viewing images of scantily dressed girls, ages 11 to 15, in modeling poses. He admitted that his actions show questionable judgment on his part. (Tr. 24-26, 28-29, 34-36; GE 2; AE B)

Applicant presented several "U Rock" awards from his current employer recognizing his contributions to the overall success of the company. He also received recognition for his five years of service in August 2020. (AE A)

Policies

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 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 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 careful weighing 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.

Under Directive ¶ E3.1.14, the Government must present evidence to establish controverted facts alleged in the SOR. Under Directive ¶ E3.1.15, an “applicant is responsible for presenting witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by applicant or proven by Department Counsel, and 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 that an 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.

Section 7 of EO 10865 provides that decisions shall be “in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned.” See *also* EO 12968, Section 3.1(b) (listing multiple prerequisites for access to classified or sensitive information).

Analysis

Guideline D, Sexual Behavior

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

Sexual behavior that involves a criminal offense; reflects a lack of judgment or discretion; or may subject the individual to undue influence of coercion, exploitation, or duress. These issues, together or individually, may raise questions about an individual's judgment, reliability, trustworthiness, and ability to protect classified or sensitive information. Sexual behavior includes conduct occurring in person or via audio, visual, electronic, or written transmission. No adverse inference concerning the 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 in this case. The following is potentially applicable:

(a) sexual behavior of a criminal nature, whether or not the individual has been prosecuted; and

(d) sexual behavior of a public nature or that reflects lack of discretion or judgment.

In approximately 1997, Applicant admitted and pleaded guilty to sexually assaulting his 11-year-old stepdaughter on multiple occasions. Between 2001 and 2015, Applicant admitted downloading and viewing on his company-issued laptop images of adult pornography and child erotica. He further admitted that his actions demonstrated poor judgment. The above disqualifying conditions apply to SOR ¶¶ 1.a and 1.b. The allegation in SOR ¶ 1.c does not fall within any disqualifying condition under this Guideline.

I have also considered all of the mitigating conditions for sexual behavior under AG ¶ 14 and considered the following potentially relevant:

(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

(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.

Applicant's sexual assaults on his 11-year-old stepdaughter occurred over twenty years ago. His viewing of adult pornography and child erotica on his company-issued laptop occurred as recently as 2015. While these dates might suggest that his actions are in the past, his admission of his ongoing fascination of and stimulation by viewing child erotica, as recently as a month before his hearing, calls into question his recent judgment. The common denominator of a continuing sexual fascination with pre-teenage girls and his past criminal acts and unauthorized computer use also involving pre-teenage girls casts doubt on his current reliability, trustworthiness, and judgment. AG ¶ 14(b) does not apply. Applicant completed the court-ordered counseling associated with his 1997 offense. He failed to corroborated his assertions that a therapist gave him a positive prognosis concerning his sexual behavior. He also failed to document any treatment he received. AG ¶ 14(e) has some application.

Guideline M, Use of Information Technology Systems

AG ¶ 39 expresses the security concern pertaining to use of information technology systems:

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. I have considered the following as potentially relevant:

(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's signing documents putting him on notice that the use of his company-issued computer was not for personal use does not raise a disqualifying condition under this Guideline. From 2001 and 2015, Applicant viewed, downloaded, and saved adult pornographic images and child erotica using his company-issued laptop in violation of C1's written prohibition to use the laptop for these purposes. The above conditions are applicable to SOR ¶ 2.b, but not to SOR ¶ 2.a.

I reviewed all of the mitigating conditions under AG ¶ 41, and I considered the following relevant:

(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.

Although some time has passed since Applicant engaged in his unauthorized action, he failed to fully accept responsibility for his actions by claiming that "someone" told him he could use his company laptop for personal use. Future recurrence cannot be ruled out. Without accepting responsibility for his actions his current reliability, trustworthiness, and judgment are called into question. AG ¶ 41(a) does not fully apply.

Guideline E, Personal Conduct

AG ¶ 15 expresses the personal conduct security concern:

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.

AG ¶ 31 describes conditions that could raise a security concern and may be disqualifying in this case. The following are potentially applicable:

(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; and

(f) violation of a written or recorded commitment made by the individual to the employer as a condition of employment.

Applicant's occasions of committing sexual abuse on his 11-year-old stepdaughter demonstrate questionable behavior and raise questions about his reliability, trustworthiness and ability to protect classified information. Likewise, his use of his company-issued laptop to view pornography and child erotica would affect his personal and professional standing. Applicant used his company-issued laptop in violation of the written company policy not to do so. I find the above disqualifying conditions applicable, although SOR ¶¶ 3.a and 3.b essentially allege the same underlying conduct. Because of this, I find for Applicant on SOR ¶ 3.a.

The guideline also includes conditions that could mitigate security concerns arising from personal conduct. I have considered all of the mitigating conditions under AG ¶ 17 and found the following relevant:

(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.

As stated under the Guideline D analysis above, because of the similarities between Applicant's continuing sexual affixation on pre-teenage girls and his past criminal and employment-ending behavior also involving pre-teenage girls, the passage of time here is not determinant. His actions continue to cast doubt on his reliability, trustworthiness, and good judgment. To some extent he has accepted responsibility for his criminal acts perpetrated on his stepdaughter. He also admitted he used poor judgment using his company-issued laptop (while also claiming he was told by someone—unverified—he could use it for personal use) to download and view pornography and child erotica. He completed court-ordered counseling and he claims he sought counseling through a 12-step program and use of a therapist, but failed to document these activities. AG ¶ 17(c) does not apply, but AG ¶¶ 17(d) and 17(e) have some application.

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 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 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 Applicant's awards, his removal from the sex offender list, and his lack of criminal charges since 1997. I weighed these factors against his conviction for sexually abusing his stepdaughter, his employment termination for violating company policy regarding computer usage, and his continuing interest in viewing sexually provocative images of pre-teenagers on his own electronic devices.

Overall the record evidence leaves me with questions and doubts about Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude Applicant failed to mitigate the security concerns under Guidelines D, M and E.

Formal Findings

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

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

Conclusion

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

Robert E. Coacher
Administrative Judge