DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
[Name Redacted]	)	ISCR Case No. 18-01224
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Michelle Tilford, Esq., Department Counsel
For Applicant: *Pro se*

03/04/2019

_____

Decision

_____

MATCHINSKI, Elizabeth M., Administrative Judge:

During a polygraph interview in June 2014, Applicant reportedly admitted accessing Internet images of nude minors starting in 2012 or 2013, and becoming sexually aroused when viewing the images and when reading erotic stories concerning minors online. Applicant admits that he viewed legal pornography on nudist-colony websites, but asserts that his access to child pornography was inadvertent and limited to two occasions. Applicant has not allayed the security concerns raised by his polygraph-interview disclosures. Clearance is denied.

Statement of the Case

On May 22, 2018, the Department of Defense Consolidated Adjudications Facility (DOD CAF) issued a Statement of Reasons (SOR) to Applicant, detailing security concerns under Guideline D, sexual behavior, and Guideline E, personal conduct. The SOR explained why the DOD CAF was unable to find it clearly consistent with the national interest to grant or continue security clearance eligibility for him. The DOD CAF took the action 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 *National Security Adjudicative Guidelines for Determining Eligibility for Access to Classified Information or Eligibility to Hold a Sensitive Position* (AG) effective within the DOD on June 8, 2017.

On June 18, 2018, Applicant responded to the SOR allegations and requested a decision based on the written record by an administrative judge from the Defense Office of Hearings and Appeals (DOHA). On July 24, 2018, the Government submitted a File of Relevant Material (FORM), consisting of six exhibits (Items 1-6). DOHA forwarded a copy of the FORM to Applicant on July 26, 2018, and instructed him to respond within 45 days of receipt. Applicant received the FORM on August 8, 2018, and he submitted a timely response that was accepted without any objections by the Government on September 14, 2018. On November 30, 2018, the case was assigned to me to determine whether it is clearly consistent with national security to grant or continue a security clearance for Applicant. I received the case assignment on December 3, 2018, and accepted Applicant's FORM response in the record as Applicant Exhibit (AE) A.

Evidentiary Ruling

Department Counsel submitted as Item 4 a June 10, 2014, report of a lifestyle polygraph interview conducted by another government agency, and as Item 6 a summary report of subject interviews of Applicant conducted for his current background investigation on July 5, 2017, on July 10, 2017, and September 5, 2017. The summary report was part of the DOD Report of Investigation (ROI) in Applicant's case. Under ¶ E3.1.20 of the Directive, a DOD personnel background report of investigation may be received in evidence and considered with an authenticating witness, provided it is otherwise admissible under the Federal Rules of Evidence. The summary report did not bear the authentication required for admissibility under ¶ E3.1.20.

In ISCR Case No. 16-03126 decided on January 24, 2018, the Appeal Board held that it was not error for an administrative judge to admit and consider a summary of personal subject interview where the applicant was placed on notice of her opportunity to object to consideration of the summary; the applicant filed no objection to it; and there is no indication that the summary contained inaccurate information. In this case, Applicant was provided a copy of the FORM and advised of his opportunity to submit objections or material that he wanted the administrative judge to consider. In a footnote, the FORM advised Applicant of the following:

> **IMPORTANT NOTICE TO APPLICANT**: The attached summary of your Personal Subject Interview (PSI) (Item 3) [sic] is being provided to the Administrative Judge for consideration as part of the record evidence in this case. In your response to this File of Relevant Material (FORM), you can comment on whether the PSI summary accurately reflects the information you provided to the authorized OPM investigator(s) and you can make any corrections, additions, deletions, and updates necessary to make the summary clear and accurate. Alternatively, you can object on the ground that

> the report is unauthenticated by a Government witness and the document may not be considered as evidence. If no objections are raised in your response to the FORM, or if you do not respond to the FORM, the Administrative Judge may determine that you have waived any objections to the admissibility of the summary and may consider the summary as evidence in your case.

Concerning whether Applicant understood the meaning of authentication or the legal consequences of waiver, Applicant's *pro se* status does not confer any due process rights or protections beyond those afforded him if he was represented by legal counsel. He was advised in ¶ E3.1.4 of the Directive that he may request a hearing. In ¶ E3.1.15, he was advised that he is responsible for presenting evidence to rebut, explain, or mitigate facts admitted by him or proven by Department Counsel and that he has the ultimate burden of persuasion as to obtaining a favorable clearance decision. While the Directive does not specifically provide for a waiver of the authentication requirement, Applicant was placed on sufficient notice of his opportunity to object to the admissibility of the interview summary report, to comment on the interview summary, and to make any corrections, deletions, or updates to the information in the report. He did not file any objections to the interview report in his rebuttal (AE A) to the FORM. Instead, he stated that the summary of the interview included as Item 6 is an accurate representation of the information he provided to the OPM investigator. Accordingly, I accepted Item 6 in evidence, subject to issues of relevance and materiality in light of the entire record.

In his rebuttal to the FORM, Applicant objected instead to the report of his polygraph interview (Item 4) as a summary of his statements from the perspective of the investigator lacking the context of the questions and any quoted statements by him. Applicant contended that the interviewer "took advantage of apparent guilt fed by Applicant, based on his personal moral code grounded in his professed religion;" a guilt not grounded in illegal activities but in having viewed any pornography. Mindful that Government officials are entitled to a presumption of regularity in the discharge of their official responsibilities,[1] I reviewed the report, but considered Applicant's concerns in determining the weight to be afforded the information in light of the evidence as a whole.

Findings of Fact

The SOR alleges under Guideline D (SOR ¶ 1.a), and cross-alleges under Guideline E (SOR ¶ 2.a),[2] that Applicant deliberately sought out and viewed sexually explicit photos of underage females on various occasions between at least 2012 and June 2014. (Item 1.) In his Answer to the SOR (Item 2), Applicant denied the conduct alleged. He indicated that the allegation is "a gross misrepresentation of information considered to be a discovery by a polygraph interviewer," who conducted "an extensive intrusion" lasting upwards of four

[1] *See e.g.*, ISCR Case No. 15-07539 (App. Bd. Oct. 18, 2018).

[2] SOR ¶ 2.a alleged "Information as set forth in subparagraphs 1.a through 1.q., above." There are no allegations 1.b through 1.q in the SOR of record.

hours where any response by him indicating inadvertent or potential engagement was interpreted as if there had been criminal activity.

After considering the FORM, which includes Applicant's Answer to the SOR (Item 2), and AE A, I make the following findings of fact.

Applicant is a 30-year-old computer software engineer. He has a bachelor's degree in computer science awarded in December 2011 and a master's degree in computer information science awarded in May 2014. (Item 5.) He has worked for his current employer, a large defense contractor, since November 2014. He has been married since April 2014, and he and his spouse have a two-year-old son. (Item 3.)

While in college, Applicant ignored known university policies regarding computer use several times. In November 2007 or 2008, he ran a penetration test with a hacking tool and by scanning the university's unblocked network traffic, was able to log onto another student's laptop and steal his passwords. A friend had bet him that it could not be done, and Applicant wanted to show him otherwise. The university disabled his student account for one semester, but Applicant got around it by using two or three other students' credentials to gain Internet access. While taking a technical writing course in the summer of 2011, Applicant asked the computer science department if he could perform a blanket sweep of the network to scan for security certificates and cookie certificates. After being denied authorization, he used his personal computer to "attack" 10 to 12 student accounts, although he did not steal or save any information from their accounts. Between 2007 and 2011, Applicant streamed movies knowing that they had been illegally downloaded by a friend. Applicant illegally downloaded computer games from various sites, and after obtaining computer software programs for trial, he used a software tool that removed the license features. (Items 4, 6.)

Applicant worked as a graduate research assistant during academic semesters from January 2012 through May 2014 while pursuing his master's degree. From June 30, 2013, to March 8, 2014, he was an intern with another government agency. An information security specialist familiar with Applicant's work indicated in June 2014 that Applicant was highly skilled in computer-related issues. (Item 5.)

In April 2014, Applicant completed a security clearance application for a top secret clearance and sensitive compartmented information (SCI) access eligibility in conjunction with his application for a sensitive position with the U.S. Government. During a polygraph pre-test interview conducted on June 10, 2014, Applicant acknowledged his misuse of computer information systems in college and his illegal downloading, streaming, or retention of audio books, music, computer games, movies, and software programs. He denied any future intent to continue downloading material protected by copyright except for books.[3]

[3] The SOR does not allege any misuse of a computer information system, so his past activities cannot be considered in disqualification. In ISCR Case No. 03-20327 at 4 (App. Bd. Oct. 26, 2006), the Appeal Board listed five circumstances in which conduct not alleged in a SOR may be considered, as follows:

When asked about Internet content concerns, Applicant reportedly volunteered that he frequented two nudist-colony websites once or twice a week from 2012 to 2013 and then with somewhat lesser frequency, about four times a month to present (June 2014); that on those websites he viewed photos of naked children under the age of 18; and that in 2013, he was redirected to a different website that contained underage pornographic images and he viewed two sexually-explicit images involving females that were around age eight or nine. Applicant reportedly indicated that he became sexually aroused when viewing nude photos of children and sometimes masturbated. On one of the websites, he reportedly viewed a beauty pageant that included females of ages 16 to 22. Applicant also indicated that he accessed through Google a website containing erotic stories, and that he read stories about minors at least 50 percent of the time. He also reportedly conducted Google searches using the keywords "young nudist" and "teenage sex." Applicant is reported to have said that he has a problem in that he wants to view pornography and to have expressed his belief that he would continue to access the nudist colony websites and read exotic stories. While he indicated that his spouse was aware of the exotic stories, no one knew about his pornography viewing. (Item 4.)

Applicant's background investigator disclosed no issues of concern from former and present professors, co-workers, and friends. They indicated that Applicant was professional and focused in his information technology work, honest and trustworthy, and involved in class and religious activities. He lived within his means and had no financial issues. (Item 5.) In August 2014, Applicant he was notified that he was no longer being offered a position with the Government. (Item 6.)

In November 2014, Applicant began working for his current employer. He started completing clearance paperwork in March 2015, but due to a mix-up, he had to complete a new Questionnaire for National Security Positions (SF 86) in August 2016. On August 9, 2016, he submitted an SF 86 on which he disclosed that he had illegally or without proper authorization accessed or attempted to access an information technology system in the last seven years. He indicated that he had "side-jacked" the personal accounts of others on the same wireless network at school "as proof of concept for a paper" without obtaining authorization, but that no action was taken against him. He also disclosed that there were some minor instances of software piracy by him in the last seven years, and that he made some modifications to gaming software. (Item 3.)

On July 5, 2017, Applicant was interviewed by an authorized investigator for the Office of Personnel Management (OPM). About his previously disclosed side-jacking of classmate accounts for a research paper, Applicant indicated that he had the permission of

---

(a) to assess an applicant's credibility; (b) to evaluate an applicant's evidence of extenuation, mitigation, or changed circumstances; (c) to consider whether an applicant has demonstrated successful rehabilitation; (d) to decide whether a particular provision of the Adjudicative Guidelines is applicable; or (e) to provide evidence for the whole-person analysis under Directive Section 6.3.

In this case, Applicant's hacking or "side-jacking" experience is particularly relevant in assessing his credibility with regard to whether his viewing of child pornography was inadvertent or intentional.

the students but not of the university's information systems department. He acknowledged that he had engaged in software piracy between 2005 and possibly 2012, but he indicated no recurrence since his marriage in 2014. He explained that he could not afford to purchase the media at the time, and he did not see his conduct as wrong. After being confronted with his hacking of another student's login credentials, Applicant admitted that he and a friend successfully hacked the account of another student who told him it could not be done. Applicant's motivation in all cases was to see if he could do it. While in high school, he had hacked into a teacher's computer and obtained tests, and he hacked into the computer system in another incident and changed the results of his examinations in an advanced placement class. (Item 6.)

When asked about his Internet access to pornographic images of children twice in 2012, Applicant explained that he was not looking for pornography but instead was doing cyber research into new hacks as a hobby. In lieu of the searched-for tutorial for hacking techniques, the pictures "popped up."[4] Applicant acknowledged that he had viewed other types of pornography that is legal, but he ceased that behavior shortly after his marriage. Applicant could not explain the reported polygraph interview statements that he became aroused when thinking of the innocence of children. He indicated that he had been asked so many questions, and he was embarrassed at the time because he had not told his spouse. He maintained that he told his spouse about the pornographic images after his polygraph. (Item 6.)

On July 10, 2017, Applicant was re-interviewed by the OPM investigator. About whether his viewing of child pornography could cause him problems with his spouse, family, employment, or legal authorities, Applicant responded that the incident was embarrassing but that he would talk about it. (Item 6.)

In response to the SOR, Applicant denied that he intentionally sought out or viewed child pornography, and stated, in part:

> The [polygraph] interviewer had misconstrued my apparent discomfort based on my distaste for the topic in general and initiated a line of questioning over an extended period of time to reword questions which had seemed designed to coerce responses, that when answered in the affirmative, would imply engagement in related behaviors. It had seemed that any response which had indicated inadvertent or potential engagement prompted interrogation and interpretation as if there had been criminal activity.

Applicant denied that any of the behaviors "actually discussed" in the polygraph interview were habitual in nature or that he would be prone to blackmail because the incidents were known to his wife, some close friends, and a couple of co-workers. He added that nothing "resembling the original incident" has recurred since he encountered the material accidentally. Applicant indicated that after he was advised of the allegations in the more recent clearance process, he was interviewed by an agent from the Federal

[4] He now claims that he "misremembered" the website containing the sexually-explicit images during his OPM interview. (AE A.)

Bureau of Investigation (FBI) agent, who "believed there to have been a significant misrepresentation of events from the polygraph."[5] Applicant expressed a willingness to undergo a psychological assessment to "substantiate [his] assertions that the allegations are a product of exaggeration and misinterpretation and that there is no risk of any deliberate occurrence of the alleged behavior." (Item 2.)

Applicant was provided a copy of the polygraph report in the FORM. In rebuttal (AE A), he indicated that "vital information had been excised from the official record to construct a misleading narrative indicating the inaccurate conclusions aligning with the accusations that [he] contests." He indicated that the interviewer asked shocking questions, and spent hours on the issue in an attempt to elicit a single positive response. While disputing the accuracy of the polygraph report, Applicant did not deny that he had visited the three websites named in the report, but he asserted that one website contained legal erotic stories, and the other two websites "contained legal depictions of nudism, defined as non-sexually explicit nude images." Applicant asserted that the interviewer took advantage of the guilt that he felt in having viewed any pornography because of his "personal moral code grounded in his professed religion." Because of his "self-induced emotional state," he felt manipulated by the investigator, who pressured him for details. Being as candid as possible, he informed the interviewer of an incident in which he believed he may have inadvertently encountered illegal sexually explicit images. Concerning his specific responses, Applicant claims that he interpreted the questions as pertaining to the websites generally and not with regard to illegal contraband. He never intended to characterize his exposure to illegal material as frequent or of interest to him.

In an attempt to reconstruct the polygraph interviewer's inquiries, Applicant acknowledged the following admissions made during his polygraph interview:

- He viewed pornography or images containing nude persons approximately once to twice a week from 2012 to 2013 and once a week to June 2014.

- He viewed images on nudist websites, which was becoming a habit that he felt was morally reprehensible.

- He became sexually aroused by an image and masturbated to ejaculation while viewing the image, although he later indicated that he acted on reading a fictional erotic story.

- He viewed images of families on nudist webpages with the ages of family members ranging from infancy to elderly.

- He viewed images of people representing themselves as underage but not intentionally.

[5] There is no report of an interview with an FBI investigator in the record. Applicant may have been referring to his interview with the OPM investigator, although in his rebuttal to the FORM (AE A), Applicant expressed his understanding that his July 2017 interviewers were with an OPM investigator, and he indicated that there was an external FBI investigation.

- He clicked on a category expected to contain teenage images but he was unsure of the actual age of the females pictured.

- He viewed websites containing questionably-related materials, *i.e*., the three named websites during his polygraph interview. About the three websites, Applicant indicated that he was asked very explicit questions that were "shocking and uncomfortable enough to find themselves excluded" from the report, and that he answered affirmatively "under the mistaken assumption that any actions should be initially construed in the most stark and worst degree and that questions intended to provide context and mollify any initial responses would be forthcoming." He denied that the statements made in the short discussions were intended to imply a habit or intentional engagement with illegal material.

- While in the photo gallery of one of the two nudist websites in 2013, he viewed a picture from the teenage category that redirected him to a different website where he looked at a pornographic image of a female around age eight or nine for about five seconds. After he closed that image, an image popped up of a female of similar age being sexually penetrated by an older male. He found it shocking and viewed it for only a few seconds.

- As of his polygraph interview in June 2014, he was hiding his involvement with pornography from everyone.

Applicant added that some of his responses to the inquiries of the polygraph interviewer may have been made "to please and perhaps impress the interviewer with stark and candid responses to demonstrate a willingness to cooperate to the greatest degree possible." Applicant denied any inference that he had a habit of viewing illegal pornography. Because he considered all forms of pornography to be morally problematic, he reduced the frequency of viewing overtime and eventually switched from images to text-based stories. Applicant submitted that his conduct was morally questionable by his own standards but not illegal, and that his inadvertent encounters with child pornography had been fully mitigated by revealing the information to his wife, to some co-workers, and to friends, including a couple of gaming friends whom he had net met in person. While acknowledging that he had previously felt guilty at having viewed pornography or nudist material, he asserted that those behaviors "now serve as a means by which [he] can empathize with others who experience the same forms of guilt about falling short on self-imposed morality." He submitted that his sexual behaviors were "strictly private and discrete." As evidence of his candor, Applicant cited his self-admitted questionable uses of computing resources "to show off and generate some measure of pride among peers about his talents with computing devices. (AE A.)

Policies

The U.S. Supreme Court has recognized the substantial discretion the Executive Branch has in regulating access to information pertaining to national security, emphasizing that "no one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484

U.S. 518, 528 (1988). 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 required to be considered 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 overall adjudicative goal is a fair, impartial, and commonsense decision. According to AG ¶ 2(a), the entire process is a conscientious scrutiny of a number of variables known as the "whole-person concept." The administrative judge must consider all available, reliable information about the person, past and present, favorable and unfavorable, in making a decision.

The protection of the national security is the paramount consideration. AG ¶ 2(b) requires that "[a]ny doubt concerning personnel being considered for national security eligibility will be resolved in favor of the national security." In reaching this decision, I have drawn only those conclusions that are reasonable, logical, and based on the evidence contained in the record. 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 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 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. 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 concerns about sexual behavior are articulated 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 for 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 report of Applicant's June 2014 polygraph interview reflects frequent access by Applicant from 2012 "to present" (*i.e.,* June 2014) of nudist websites where he viewed nude images of persons of all ages, including females that clearly appeared to be underage because of their physical development or were represented as being underage. Applicant is reported to have admitted viewing a photo gallery of teenagers on one of the nudist websites and becoming sexually aroused by the images. Regarding the other nudist-colony website, he viewed a naked beauty pageant that included females represented to be 16 to 22 years old. He is also reported to have conducted Google searches using the keywords "young nudist" and "teenage sex," although he indicated that the images accessed did not constitute child pornography because they were accompanied with a warning from Google about the illegality of underage pornographic material.

Applicant submits that the interviewer constructed a misleading narrative from his responses to make it appear that he intentionally sought out sexually-explicit photographs of underage females. He contends that the interviewer took advantage of his emotional distress in having viewed pornography and nudist material against his moral code and religious beliefs. However, Applicant also indicated in rebuttal that he attempted to "please and perhaps impress the interviewer with stark and candid responses."

Government officials are entitled to a presumption of regularity in good faith in the discharge of their official responsibilities. *See* ISCR 15-07539 (App. Bd. Oct. 18, 2018). While the circumstances of a polygraph interview can be somewhat stressful, there is no evidence that the polygraph interviewer deliberately misrepresented what Applicant told him. Applicant does not dispute that he accessed websites containing pornographic images and that he became sexually aroused, although primarily when reading erotic stories online. Access to adult pornography may be viewed as morally repugnant by some, but the DOD is not in the position of passing judgment on such activities unless they are shown to be illegal or contrary to policy (e.g., using a government-issued computer, access during duty hours, in circumstances showing a lack of discretion), or present an unacceptable risk of exploitation, pressure, or duress. In that regard, Applicant detailed two instances where he observed underage females in sexually-explicit acts or poses. His claim that the access was completely accidental is of suspect credibility, given his knowledge of computer systems in general (he proved to be a successful hacker in college) and other admissions during his polygraph interview that he had conducted Internet searches for "teenage sex" and having viewed images of underage females on nudist websites. With regard to his access to pornographic images involving underage females, he acknowledged in June 2014 that no one was aware that he had viewed any pornographic images. Disqualifying conditions AG ¶ 13(a), "sexual behavior of a criminal nature, whether or not the individual has been prosecuted," AG ¶ 13(c), "sexual behavior that causes an individual to be vulnerable to coercion, exploitation, or duress," and AG ¶ 13(d), "sexual behavior of a public nature or that reflects a lack of discretion or judgment," apply to a greater or lesser

extent. The evidence of his access to sexually-explicit child pornography is limited,[6] but he also hid it from his family and friends.

The burden is on Applicant to mitigate the negative implications for his judgment raised by his sexual behavior and his concealment of that sexual behavior. Two mitigating conditions under AG ¶ 14 could apply in this case.[7] They are:

> (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
>
> (c) the behavior no longer serves as a basis for coercion, exploitation, or duress.

Application of the aforesaid mitigating conditions depends on whether Applicant is to be believed when he asserts that there has been no recurrence since the instances that occurred in 2012, and that he has informed his spouse, friends, and some co-workers about his access to child pornography. Applicant presented no statements from his spouse or others who could corroborate that they know about his viewing of pornography or erotic stories involving minors. His credibility suffers to the extent that he provided discrepant accounts of the circumstances involving his access to child pornography. During his OPM interview in July 2017, he claimed that he was doing cyber research into new hacks "as a hobby of learning and the pictures were there." In June 2014, he named the nudist website (which he regularly viewed and had intentionally accessed to view a picture from the teenage category) that redirected him to the website where he viewed the sexually-explicit images involving children. He now claims that he "misremembered" the website containing the sexually-explicit images during his OPM interview. While the passage of time could diminish his recollection, he did not explain how child pornography would have "popped up" on a website for a computer-hacking tutorial.

Applicant's efforts to discredit the polygraph report with claims that the interviewer took advantage of his emotional distress, asked shocking questions, and spent hours on the issue in an attempt to elicit a single positive response, do not indicate reform. Applicant's assertion that he answered the polygraph interviewer's questions in the affirmative under the mistaken assumption that any action should be construed in the most stark and worst degree possible is contradicted by his assertion that he gave stark but also candid responses to demonstrate his willingness to cooperate. Applicant's evidence is insufficient to overcome the sexual behavior security concerns.

---

[6] Regarding the knowing access of child pornography with intent to view, which is punishable under 18 U.S.C. § 2252A, it is an affirmative defense if the alleged child pornography was produced using no minors or if the person had less than three images of child pornography, and promptly and in good faith took reasonable steps to destroy the image or reported the matter to a law enforcement agency and afforded the agency access to the image.

[7] Applicant's case for applicability of AG ¶ 14(d), "the sexual behavior is strictly private, consensual, and discrete," ignores the fact that child pornography is not consensual, even if he accessed the pornographic images in the privacy of his own home.

Guideline E: Personal Conduct

The security concerns about personal conduct are articulated 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.

Applicant's sexual behavior, as detailed under Guideline D, raises considerable concerns about his judgment generally under AG ¶ 15 and is the type of conduct contemplated within disqualifying condition AG ¶ 16(e), which provides:

> (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.

Similar to AG ¶ 14(b) under Guideline D, the personal conduct guideline also provides for mitigation when the offense was so infrequent or occurred so long ago to no longer be of security concern. AG ¶ 17(c) provides:

> (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.

For the reasons addressed under Guideline D, concerns also persist about Applicant's judgment, reliability, and trustworthiness under Guideline E. He has yet to persuade me that his poor judgment in accessing child pornography is not likely to recur or that it is no longer a source of vulnerability for him. Applicant's uncorroborated assertion that his spouse, friends, and some co-workers are aware of his sexual behavior falls short of establishing AG ¶ 17(e), "the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress." The record contains no information about what they know, if anything, about his access to illegal sexually-explicit images.

Applicant's case for mitigation under AG ¶ 17(f), "the information was unsubstantiated or from a source of questionable reliability," is largely without merit. The information of security concern was provided by Applicant, who admitted to the polygraph interviewer that he had access to sexually-explicit images of children, and that he had conducted Internet searches using the term "teenage sex." Without the opportunity to observe Applicant's demeanor and question him about his access to pornography, it is

particularly difficult to find that his access to child pornography was inadvertent. The personal conduct security concerns are not adequately mitigated.

Whole-Person Concept

In assessing the whole person, the administrative judge must consider the totality of an applicant's conduct and all relevant circumstances in light of the nine adjudicative process factors in AG ¶ 2(d). The analyses under Guidelines D and E are incorporated in my whole-person analysis. Some of the factors in AG ¶ 2(d) were addressed under those guidelines, but some warrant additional comment.

Applicant detailed a pattern of access to pornography that appears to have been legal for the most part. However, he accessed sexually-explicit images of underage females at least twice and conducted Internet searches using the term "teenage sex." Applicant may well have been "shocked" by what he saw, but it is also difficult to believe that his access to child pornography was inadvertent. He was a frequent viewer of websites where he sought out images of nude teenage females for sexual arousal. He has considerable computer knowledge and skills and knew, or should have known, to avoid questionable websites and links where he risked access to illegal pornography.

The security clearance adjudication involves an evaluation of an applicant's judgment, reliability, and trustworthiness in light of the security guidelines in the Directive. *See* ISCR Case No. 09-02160 (App. Bd. Jun. 21, 2010). It is well settled that once a concern arises regarding an applicant's security clearance eligibility, there is a strong presumption against the grant or renewal of a security clearance. *See Dorfmont v. Brown*, 913 F. 2d 1399, 1401 (9th Cir. 1990). For the reasons noted above, I am unable to conclude that it is clearly consistent with the national interest to grant Applicant access to classified information.

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
Subparagraph 1.a:	Against Applicant
Paragraph 2, Guideline E:	AGAINST APPLICANT
Subparagraph 2.a:	Against Applicant

Conclusion

In light of all of the circumstances, it is not clearly consistent with the national interest to grant Applicant's eligibility for a security clearance.

_____
Elizabeth M. Matchinski
Administrative Judge