DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 11-14005
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Daniel F. Crowley, Esq., Department Counsel
For Applicant: Mark S. Zaid, Esq.

12/02/2013

Decision

O'BRIEN, Rita C., Administrative Judge*:*

Based on a review of the pleadings, exhibits, and testimony, I conclude Applicant has mitigated the security concerns raised under the guidelines for sexual behavior and personal conduct. His request for a security clearance is granted*.*

Statement of the Case

On April 25, 2013, the Department of Defense (DOD) issued to Applicant a Statement of Reasons (SOR) that detailed security concerns under Guideline D (sexual behavior) and Guideline E (personal conduct). This action was taken under Executive Order 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; and the Adjudicative Guidelines (AG) implemented by the Department of Defense on September 1, 2006*.*

In his May 10, 2013 Answer to the SOR, Applicant denied the allegations under Guidelines D and E. The Defense Office of Hearings and Appeals (DOHA) issued a Notice of Hearing on July 23, 2013. At the August 14, 2013 hearing, I admitted six Government exhibits into evidence (GE 1-6). Applicant testified, and presented the testimony of four additional witnesses. He also offered 12 exhibits, admitted into evidence as AE A-L. DOHA received the transcript of the hearing (Tr.) on August 26, 2013.

Findings of Fact

After a thorough review of the pleadings and the evidence, I make the following findings of fact.

Applicant, 38 years old, has been married for ten years and has a daughter and son, five and seven years old, respectively. He earned a bachelor's degree in 1997, and a master's degree in 1999, both in industrial and systems engineering. He worked at federal agencies during college, and was first granted a security clearance in approximately 1994. He has worked for the same defense contractor since 2003 and holds the position of principal information systems engineer. (GE 1; AE A; Tr. 69, 89-95)

The SOR alleges that, between 1999 and 2004, Applicant intentionally accessed child pornography by downloading images of underage females, and used a file-sharing program called Kazaa to download images and videos of underage females. Applicant testified that he has never intentionally downloaded child pornography. (Tr. 95)

Applicant started viewing pornography in his teens. From the mid-1990s, when he attended college, until 2004, he searched for, downloaded, and viewed adult pornographic material, and maintained a collection on his personal computer. It consisted primarily of images, with a few videos. He viewed his collection from several times per week to once every few months. He never purchased pornographic material. (GE 3, 6; Tr. 95-100, 106)

Applicant allowed his wife and friends access to the pornographic images on his computer. During parties at his home both during and after college, male and female friends looked at his extensive collection of approximately 10,000 images. They were free to look at any of his files, and he did not restrict their perusal of folders on his computer. His wife and two of his friends testified that they were present during these events, viewed the images, and saw no material that they believed to be child pornography.[1] (Tr. 32-39, 57-60, 120-122)

[1] The federal statute at 18 U.S.C. §2256 defines child pornography as the visual depiction of a minor engaged in sexually explicit conduct. *See also* Department of Justice, "Citizen's Guide to U.S. Federal Law on Child Pornography." (AE J, K)

In about 1999, Applicant started using a peer-to-peer (P2P) software program[2] called Kazaa. Downloading pornography from the internet was slow at the time and he believed Kazaa would enable faster downloading than using the internet. The software allowed users to share files, but did not allow them to view the material in the file before downloading it. Applicant testified that the file names were often inaccurate or misleading, and he would receive material he did not want to view. For instance, using Kazaa, he downloaded a file, not realizing it consisted of a video of prepubescent girls playing at what Applicant guessed was a nudist camp. He was disturbed by the video. He testified that he never, even inadvertently, saw any other images or videos of children of that age. He told his wife about the video, and deleted it. (GE 2, 3, 6; AE H; Tr. 81-82; 100-107, 115-116)

Applicant admits that while seeking legal adult pornography, he inadvertently came across images of child pornography on rare occasions. Sometimes months to years passed between such instances of such viewing. He testified, ". . . I deliberately took specific measures to try to avoid unlawful and, to me, disturbing content. . . " In his October 30, 2005 affidavit, signed under penalty of perjury, Applicant said,

> I will state from the outset and emphatically that during the period when I perused internet pornography, I specifically took intentional steps to avoid either viewing or collecting illegal, or potentially illegal, materials. To the extent that I may have inadvertently encountered unlawful pornography, I deleted those images immediately.

Among the steps Applicant took were checking that the website had disclaimers stating the models were of legal age and complied with federal law, and providing contact information to verify the claim. He also used U.S.-based sites "that prominently display their stated policies against illegal porn and their promised compliance with applicable statutes." He used websites that, at the time, offered free sample images which he believed indicated they were legitimate sites. He also reviewed thumbnail images on websites before downloading to ensure they were not underage models. In 2001, he stopped using Kazaa because of his inability to pre-screen the material in the files. (GE 3, 6; Tr. 100-107, 112)

In 2004, as part of his security investigation by another government agency (OGA), Applicant underwent two polygraph examinations and an additional interview. The polygrapher for the OGA asked him about his use of pornography. Applicant stated that the images were of adult women. When asked about viewing child pornography, Applicant realized that, even though he had not sought child

[2] Peer-to-peer (P2P) software allows file-sharing among P2P users. It allows User A to access designated files on User B's computer and download the files to User A's computer. Only the file names on User B's computer are visible to User A; the content of the file is not visible until it is downloaded to User A's computer. The software also allows User B, and other P2P users, to view and download designated files residing on User A's computer. *See* http://www.techterms.com/definition/p2p.

pornography, he had probably seen “false positives” -- women who claimed to be adults but were not legal age. The polygrapher asked for an estimate of how many such images he could have seen. Applicant replied that, hypothetically, it could be from zero percent to the low single digits. Applicant said the polygrapher claimed his estimates were too low. Applicant testified the polygrapher continued to increase the percentage of underage females Applicant could have hypothetically viewed to four percent, to seven percent, and higher. He did not disclose to Applicant the final percent he believed Applicant viewed. However, the OGA denial letter states that Applicant estimated seeing 3,500 images of child pornography during the 1999 to 2004 period, which would indicate the polygrapher used a figure of 35 percent. Applicant believes, “When I informed the interviewer that I may have inadvertently viewed pornographic images of underage individual who represented themselves as adults, the interviewer took this statement as an admission of viewing child pornography. . .” Applicant believes the polygrapher confused the facts that Applicant provided about his actual viewing habits, with the figures raised in the hypothetical discussion of possible percentages of underage models viewed. In his 2005 affidavit, Applicant stated, “I have never sought or knowingly downloaded or kept illegal pornographic images.” He also stated, “I have certainly never encountered thousands, much less hundreds, of illegal images during the period in question.” (GE 3, 6; Tr. 107-114, 133)

Based on the 2004 interviews, the OGA denied Applicant's access to classified information in a letter dated May 2005. The letter stated that Applicant had admitted downloading child pornography multiple times between 1999 and 2004. The letter stated that Applicant admitted the pornography showed females 8 to 18 years of age in provocative poses or engaged in sexual activity. He testified that he believed the OGA’s reference to females between 8 and 12 years of age referred to the nudist camp video. The letter also stated Applicant estimated he had viewed this type of pornography “at least 3,500 times from 1999 to 2004 . . .” It said that Applicant stated, while engaged in this activity, he gratified himself sexually “. . . on at least one, but no more than three occasions.” Applicant appealed the agency’s decision. His denial was affirmed in 2008 when OGA noted that the facts were sufficient to deny access; the letter did not discuss those facts. After a second appeal, Applicant was denied in 2011, in a letter that upheld the previous decision, without further explanation. (GE 2, 4, 5, 6; Tr. 134-135)

Applicant's supervisor and facility security officer became aware of the OGA denial in 2004 or 2005. Applicant is unsure if they were aware of the specific underlying reasons. Following the denial, his supervisor retained Applicant in his position, promoted him in 2005, and again in 2008. Applicant testified that, because his family and friends knew of his actions, he was not vulnerable to coercion. (Tr. 134-137)

In his 2005 statement, Applicant cited information in the polygrapher’s report that was inaccurate: He stated that “only negative information is reported.” He noted, “I am especially troubled that nowhere in the report is mention made of my near-zero floor estimate.” He also stated, “In fact, figures like 4%, 7%, 5%, and 15% are

misconstrued as lower figures. Furthermore, on an incident basis (as is reflected in the record), the frequency with which I could recall potentially problematic files (rarely), does not sync at all with the figure [OGA] asserts." The polygrapher's report that Applicant referenced, or any other information about what transpired at Applicant's polygraph interview, is not included in the Government's evidence. (GE 3)

In the October 30, 2005 affidavit, Applicant stated, "I can state categorically, and without hesitation, that at no time did I ever seek, intentionally or otherwise, to obtain unlawful pornographic images. I never knowingly downloaded unlawful images nor maintained storage of any unlawful images." He also stated, "I categorically deny the [OGA] assertion that I admitted to or ever masturbated to underage pornography." In the same affidavit, Applicant stated he had not downloaded any pornography from the internet since 2004 and that he removed all pornography files from his computer between 2004 and 2005. He testified that he does not frequent pornography websites, and no longer has pornography on his home computer. He has not had treatment or counseling and had no difficulty ending his internet pornography use. (GE 3; GE 6; Tr. 118)

Applicant's wife testified that Applicant has been open about using pornography, and disclosed it about a month after they met in 1998. They have shared a home since 2001, and were married in 2003. They have shared one home computer, and Applicant never tried to hide any files on the computer or restrict her access. They password-protected their computer only after they had children, and they share the password. His wife has reservations about pornography. She did view the pornography on their computer several times over the years, but never saw imagery she thought was out of the ordinary or any images she would consider child pornography. (Tr. 67-88)

Applicant's wife testified that on the day of Applicant's polygraph in 2004, he returned home concerned that the polygrapher did not understand his statements and was accusing him of engaging in actions he did not say he did. The following year, on the day he received the OGA denial letter, he shared the OGA letter with her. She felt frustrated because "the allegations were completely against anything that I know of [Applicant]." At that time, they discussed his use of pornography. She opined that it was causing difficulties with his career. She testified that, in 2005, "[Applicant] deleted the materials on his computer and stopped searching for new porn." She independently checked the computer's browser history and hard drive about two months after the OGA denial in 2005, and found no pornographic images on it. She also checked it twice between 2005 and 2013 and again found no pornographic images. She does not believe he has pornographic images stored in any other location because they have always had an open and honest relationship. She and Applicant shared a single computer during the time period of 1999 to 2004, and since then. They each have access to all folders and data stored on their home computer. In 2005, Applicant's wife submitted to OGA an affidavit signed under penalty of perjury in which she stated that she and Applicant shared a computer for at least the previous five years, that she had

seen the pornography stored on the computer, and that she had ". . . not viewed any material that could have been mistaken for child pornography." (GE 3; Tr. 67-88)

Applicant provided expert testimony by an attorney who is a published author in the field of online adult pornography. He has specialized in computer forensics for the past 14 years. He has been hired by the Department of Justice as an expert on the Child Online Protection Act. He has lectured to bar associations and state and federal public defender programs on child pornography creation and distribution and P2P programs. He has worked in the area of obscenity violations and child pornography violations for 10 to 12 years. He has testified as an expert in related court cases, and provided expert reports in other cases. He was engaged in intensive research about the online adult pornography industry during the 1999 to 2004 time period. The witness explained that federal law, specifically, 18 U.S.C §2257, requires companies that provide online adult pornography to maintain records affirming that the models on their sites meet the legal age requirements. (AE C-E; Tr. 138-205)

Based on his review of the pleadings and evidence in Applicant's case**,** the witness testified that Applicant used adult sites that are well-established, have been operating for many years, and have strong financial incentives to comply with the law. The expert opined that the companies that operate these sites are unlikely to jeopardize their business operations by engaging in criminal use of minor females. In addition, if they were to use minors, they would be unlikely to succeed in violating the law because such sites use domain names, which allow them to be easily tracked and monitored for violations. (Tr. 160-161, 185)

The expert also reviewed the search terms Applicant used and found them to be "generic" and "vanilla." During the time period in question, they were ". . . very unlikely to have produced any child pornography results at all. . . They would not have been terms that would have been fetishistic enough to produce child pornography" and were not the terms that commonly lead to child pornography sites. He also reviewed the search methods Applicant used, and opined that they are unlikely to lead to the "specialized locales where child pornography is located." He testified that the steps Applicant took to avoid downloading child pornography were legitimate and reasonable ways to avoid viewing or downloading such material, especially when he stopped using Kazaa in 2001. (Tr. 173-175, 190-191*)*

Applicant's father completed 40 years in service to the OGA in question, and held a top secret clearance with SCI access. He submitted a statement describing his close relationship with his son. He describes Applicant as a trustworthy person whose strong moral character does not track with the description portrayed by the OGA polygrapher. He stressed the trust placed in Applicant by his employers, and his unblemished record while he held a security clearance. (AE F)

Applicant's friend of 23 years testified. He works for a defense contractor and has held a security clearance for about 15 years, the last nine years at the TS/SCI

level. He has undergone polygraph examinations. In about 2005, he was aware that Applicant was having problems with his clearance. The witness is also aware of the current SOR allegations, and has read the SOR and Applicant's exhibits. He is familiar with the pornographic imagery Applicant had stored on his home computer in the past. At a party in college in about 1995 or 1996, and once at a party in Applicant's apartment in about 2001, the witness and others at the party viewed Applicant's pornography collection. Applicant was aware they were viewing it, and made no attempt to stop them or prevent their access to any folders. The witness saw no images of females who appeared to be minors. The witness has four children who are often present during social events with Applicant's family, and the witness has no hesitation about them being around Applicant. He characterized Applicant as ethical person and "morally straight." (Tr. 25-51)

Another friend of more than 20 years testified. He is a network engineer who currently holds a top secret security clearance. In the past, Applicant shared his difficulties with the OGA denial of his clearance. More recently, he shared the SOR. The witness viewed Applicant's pornography collection in the mid-1990s and in about 2000, during parties at Applicant's house. Numerous other people were also looking at the collection, and all had free access to all folders on Applicant's computer. The witness saw only adult models, and no images that he thought were underage females. He has two young daughters and has no concerns for their wellbeing when they are at Applicant's home. He described Applicant as an intelligent man, a caring father, respectful of others' feelings, willing to help his friends, and trustworthy. (Tr. 51-66)

Applicant is involved in his community, where he active in his church and volunteers as his son's cub scout leader. His performance evaluations from 2009 through 2012 praise his technical and communications skills, and describe him as a highly valued employee, and an integral part of the leadership team. His employer has presented him with several professional achievement awards. Between 2001 and 2013, Applicant published numerous technical papers and articles, and was a speaker at technical conferences. The manager of the corporate security service center submitted a statement that Applicant had not been cited for security violations, incidents, or infractions during his 10 years of employment. (AE A, B, G, L; Tr. 83, 89-95)

Policies

Each security clearance decision must be a fair and commonsense determination based on examination of all available relevant and material information, and consideration of the pertinent criteria and adjudication policy in the AG.[3] Decisions must also reflect consideration of the factors listed in ¶ 2(a) of the Guidelines, commonly referred to as the "whole-person" concept. The presence or absence of a disqualifying or mitigating condition does not determine a conclusion for or against an applicant. However, specific applicable guidelines are followed whenever a case can

[3] Directive. 6.3.

be measured against them as they represent policy guidance governing the grant or denial of access to classified information. In this case, the pleadings and the information presented by the parties require consideration of the security concerns and adjudicative factors addressed under Guideline D (sexual behavior) and Guideline E (personal conduct).

A security clearance decision is intended only to resolve the question of whether it is clearly consistent with the national interest[4] for an applicant to either receive or continue to have access to classified information. The Government bears the initial burden of producing admissible information on which it based the preliminary decision to deny or revoke a security clearance for an applicant. Additionally, the Government must be able to prove controverted facts alleged in the SOR. If the Government meets its burden, it then falls to the Applicant to refute, extenuate or mitigate the Government's case. Because no one has a "right" to a security clearance, an applicant bears a heavy burden of persuasion.[5] A person who has access to classified information enters into a fiduciary relationship with the Government based on trust and confidence. Therefore, the Government has a compelling interest in ensuring each applicant possesses the requisite judgment, reliability, and trustworthiness of one who will protect the national interests as her or his own. The "clearly consistent with the national interest" standard compels resolution of any reasonable doubt about an applicant's suitability for access in favor of the Government.[6]

Analysis

Guideline D, Sexual Behavior

AG ¶ 12 expresses the security concern about personal conduct:

> Sexual behavior that involves a criminal offense, indicates a personality or emotional disorder, reflects lack of judgment or discretion, or which may subject the individual to undue influence or coercion, exploitation, or duress can raise questions about an individual's reliability, trustworthiness and ability to protect classified information. . . .

I have considered the following conditions under AG ¶ 13 that could raise security concerns and may be disqualifying:

---

[4] *See Department of the Navy v. Egan*, 484 U.S. 518 (1988).

[5] *See Egan,* 484 U.S. at 528, 531.

[6] *See Egan;* AG ¶ 2(b).

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

(c) sexual behavior that causes an individual to be vulnerable to coercion, exploitation, or duress; and

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

Applicant maintained a collection of adult pornography that contained thousands of images and some videos. Pornography involving women 18 or over is legal and ordinarily does not raise a security concern. However, while discussing hypothetical situations during a polygraph examination, Applicant stated that a small percentage of the pornography he viewed could have been of women who, unknown to him, were not legal age. The polygrapher took Applicant's discussion of hypotheticals as an admission that he had intentionally sought and viewed female models who were under the legal age. Applicant denies stating to the polygrapher that he intentionally sought out child pornography.

The Government's evidence includes the letters in which the OGA denied Applicant's security clearance. The first letter provides one paragraph stating that Applicant admitted to viewing images of child pornography about 3,500 times between 1999 and 2004, showing females from 8 to 18 engaged in sexual activity, and that he masturbated using these images one to three times. The remaining information in the letter is procedural. The other two denial letters present no additional information about the interview or how the decision was reached. The SOR allegations stem from the paragraph in the first letter. Applicant denies the admissions ascribed to him, and the record contains no facts or details about how the polygrapher arrived at his conclusions that Applicant had admitted to viewing child pornography, or how he arrived at a figure of 3,500 images.

The record presents conflicting evidence. The initial OGA denial letter states that Applicant admitted he downloaded, viewed, and masturbated using child pornography. Applicant denies admitting to intentionally engaging in such activity. In his affidavits, Applicant noted several parts of the polygrapher's interview report that were inaccurate. However, the polygrapher's report, or any information about what transpired at Applicant's polygraph interview, is not included in the evidence offered by the Government. Without the polygrapher's report, I cannot evaluate what occurred at the interview--the questions asked of Applicant, and the answers he gave--to evaluate the basis on which the polygrapher decided that Applicant had admitted to illegal acts.

The denial letters presented by the Government constitute substantial evidence. There is no evidence or implication that the polygrapher engaged in irregular behavior.[7]

[7] ISCR Case No. 11-07509 at 5, footnote 3 (App. Bd. June 25, 2013), "Official records are presumed to be reliable by virtue of the agency's duty of accuracy and the high probability that it has satisfied that

The conclusions in the letters are potentially disqualifying, and I have seriously considered them. However, the Government's evidence must be considered in light of the contrary evidence in the record. Applicant has also presented substantial evidence: his frank and credible testimony denying intentional use of child pornography; his affidavits stating that he did not admit to intentionally viewing child pornography; his wife's affidavits and testimony that she had accessed their computer for years and never found child pornography during random checks; the unlikelihood that he would give others free access to his computer if it contained any images that could be interpreted as child pornography; his friends' testimony about their personal knowledge of the type of pornography he had at the time, and of their knowledge of his habits and character; the expert's testimony that Applicant took reasonable steps to protect himself from viewing child pornography; and the evidence showing Applicant's long history of successfully holding a security clearance. Weighing the substantial evidence presented by both parties, as well as the favorable and unfavorable evidence in the file,[8] I find Applicant carried his burden to show that he did not intentionally download and view underage females or any material that would constitute child pornography.[9] As Applicant did not intentionally view or download child pornography, he did not engage in criminal activity, and AG ¶ 13(a) does not apply.

Applicant found the questions posed by the polygrapher to be embarrassing, and testified that it would have been upsetting if his employer had known about his pornography use. Applicant's pornography collection created a vulnerability to exploitation, and AG ¶ 13 (c) applies.

Between 1999 and 2001, Applicant used a P2P file-sharing program that prevented him from reviewing material before downloading it. As a result, he was unable to determine beforehand if material he downloaded contained illegal pornography. One file he downloaded using P2P software was a video that showed naked children playing at a nudist camp. He was disturbed by the video, told his wife about it, and deleted it. For two years, Applicant engaged in the risky behavior of using file-sharing software that exposed him to the possibility of downloading and viewing illegal pornography. Applicant's conduct reflected a lack of judgment, and AG ¶ 13(d) applies.

---

duty." [Citations omitted] *See also,* ISCR Case No. 11-03452 at 4 (App. Bd. June 12, 2013) in which the Appeal Board found that Clearance Decision Statements from OGAs are admissible as substantive evidence in DOHA hearings. However, the evidence here does not include a Clearance Decision Statement.

[8] *See generally,* ISCR Case No. 10-07794 at 2 (App. Bd. Oct. 4, 2011) discussing the judge's obligation to determine the facts, after taking into account and resolving any discrepancies raised by the evidence.

[9] Once the Government presents substantial evidence of security concerns, an applicant bears the burden of presenting evidence to mitigate them. Directive ¶ E3.1.15.

AG ¶14 provides the following mitigating conditions:

> (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 good judgment;
>
> (c) the behavior no longer serves as a basis for coercion, exploitation, or duress; and
>
> (d) the sexual behavior is strictly private, consensual, and discreet.

Although Applicant frequently used pornography between the 1990s and 2004 or 2005, he took steps to avoid inadvertently downloading child pornography. In 2004 or 2005, he deleted all of the pornographic material from his computer. His pornography use is not recent, as it has been eight years since he removed the pornography from his computer and stopped accessing adult online pornography. It has been 12 years since he stopped using the P2P software that exposed him to the possibility of downloading child pornography. Applicant's conduct is not recent, and his current trustworthiness and judgment are not in question. AG ¶ 14(b) applies.

Applicant was open with his wife and friends about his pornography since the 1990s. He gave them free access to his computer, and did not restrict their use of any files or folders. His employer is aware that his security clearance was denied by OGA, and believed in his trustworthiness to the extent that he was retained in his position and promoted. Applicant is not subject to exploitation based on his maintaining a legal pornography collection eight years ago. His use of adult pornography was discreet and private, as it occurred in his own home, on his own computer. The record contains no evidence indicating that his conduct was public, flagrant, or indiscreet. AG ¶ 14(c) and (d) apply.

Guideline E (Personal Conduct)

AG ¶ 15 expresses the security concern about personal conduct:

> 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 information. . .

The Guideline E allegations implicate the following disqualifying conditions under AG ¶ 16:

> (c) credible adverse information **. . .** which, when considered as a whole, supports a whole-person assessment of questionable judgment,

> untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the person may not properly safeguard protected information; and
>
> (e) personal conduct, or concealment of information about one's conduct, that creates a vulnerability to exploitation, manipulation, or duress, such as (1) engaging in activities which, if known, may affect the person's personal, professional, or community standing. . .

As discussed *supra*, Applicant collected, downloaded, and viewed legal adult pornographic material, which does not raise a security concern. However, when he engaged in this activity from 1999 to 2004, and especially when he used P2P software from 1999 to 2001, he placed himself at risk of inadvertently viewing child pornography, which raises a concern about his judgment and the effect his actions could have on his personal and professional standing. AG ¶¶ 16(c) and (e) apply.

Under AG ¶ 17, the following mitigating conditions are 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 . . . taken other positive steps to alleviate the . . . factors that caused the untrustworthy, unreliable, or other inappropriate behavior, and such behavior is unlikely to recur; and
>
> (e) the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress.

During the period at issue, 1999 to 2004, Applicant downloaded and viewed legal pornography. However, he mitigated the possibility of downloading child pornography by frequenting established sites, checking the site's disclaimers regarding adherence to federal law, and previewing thumbnails to avoid questionable material. He took a key step in 2001, when he discontinued his use of the Kazaa P2P software that presented a risk of exposure to child pornography. Moreover, in 2004, he stopped downloading all pornographic material, and between 2004 and 2005 he deleted all of the pornographic material from his computer. Applicant's actions reduced and then eliminated the risk of exposure to child pornography. His conduct is not recent: it occurred 8 to 12 years ago and does not cast doubt on his current reliability, trustworthiness, or good judgment. Applicant's past use of pornography could not be used to exploit him because his employer has been aware of the OGA denial since 2005, and because he was open with his family and friends throughout the years about his collection, about the OGA denial, and the SOR. He did not prevent his wife or his

friends from viewing the images on his computer, and they were familiar with the materials. AG ¶¶17(c), (d) and (e) apply.

Whole-Person Analysis

Under the whole-person concept, an administrative judge must evaluate the applicant's security eligibility by considering the totality of an applicant's conduct and all the circumstances. An administrative judge should consider the nine adjudicative process factors listed at AG ¶ 2(a):

> (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.

AG ¶ 2(c) requires that 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. Under the cited guidelines, I considered the potentially disqualifying and mitigating conditions in light of all the facts and circumstances surrounding this case.

Applicant admits that he maintained an extensive collection of pornography, but denies that he intentionally sought, downloaded, or viewed child pornography. When he underwent a polygraph by OGA, he engaged in hypothetical scenarios with the polygrapher in which he projected that he could have unintentionally downloaded a low percentage of pornography that included underage females. He believes the polygrapher mistakenly conflated Applicant's hypothetical figures with admissions that he intentionally downloaded and viewed child pornography. The record does not contain a report of Applicant's interviews, a clearance decision statement, or any documents that provide the facts or details that underlie the polygrapher's conclusion that Applicant admitted to accessing illegal material.

I found Applicant's testimony that he never downloaded child pornography to be credible. Applicant's wife and friends had free access to his collection, and they credibly testified that they never encountered child pornography. He took reasonable steps to avoid illegal pornography. He used search terms that the expert testified would be unlikely to lead to the specialized areas that include child pornography. It has been eight years since Applicant deleted all pornography from his computer. It has been 12 years since he has used the file-sharing program that increased the risk of inadvertently downloading child pornography. Given the effect the use of legal pornography has had on his career, it is unlikely his past behavior will recur.

The Government provided substantial evidence in its OGA denial letters. Applicant also provided substantial evidence which rebutted the Government's evidence: his affidavits signed under penalty of perjury stating that he did not admit to intentionally viewing child pornography; his credible testimony denying that he intentionally accessed child pornography; his wife's affidavits and testimony; his friend's testimony of their knowledge of his habits and character; the expert's testimony; the evidence showing Applicant's successful work history, promotion, commendations; and his history of successfully holding a security clearance.

The record evidence satisfies the doubts raised about Applicant's suitability for a security clearance. For all these reasons, I conclude Applicant has mitigated the security concerns raised by the cited adjudicative guidelines.

Formal Findings

Paragraph 1, Guideline D	FOR APPLICANT
Subparagraphs 1.a – 1.b	For Applicant
Paragraph 2, Guideline E	FOR APPLICANT
Subparagraph 2.a	For Applicant

Conclusion

In light of all of the circumstances presented by the record in this case, it is clearly consistent with the interests of national security to allow Applicant access to classified information. Applicant's request for a security clearance is granted**.**

RITA C. O'BRIEN
Administrative Judge