



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



In the matter of:)
)
-----) ISCR Case No. 11-07509
)
Applicant for Security Clearance)

Appearances

For Government: Alison O’Connell, Esquire, Department Counsel
For Applicant: Jon L. Roberts, Esquire

02/11/2013

Decision

GALES, Robert Robinson, Administrative Judge:

Applicant mitigated the security concerns regarding sexual behavior, criminal conduct, use of information technology systems, and personal conduct. Eligibility for a security clearance and access to classified information is granted.

Statement of the Case

On May 12, 2009, Applicant applied for a security clearance and submitted an Electronic Questionnaire for Investigations Processing (e-QIP) version of a Security Clearance Application (SF 86).¹ The Department of Defense (DOD) issued a Statement of Reasons (SOR) to him on April 4, 2012, under Executive Order 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended and modified; DOD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended and modified (Directive); and the *Adjudicative Guidelines for Determining Eligibility For Access to Classified Information* (December 29, 2005) (AG) applicable to all adjudications and other determinations made under the Directive, effective September 1, 2006. The SOR alleged security concerns under

¹ Item 5 (SF 86, dated May 12, 2009).

Guidelines D (Sexual Behavior), J (Criminal Conduct), M (Use of Information Technology Systems), and E (Personal Conduct), and detailed reasons why the DOD adjudicators were unable to find that it is clearly consistent with the national interest to grant or continue a security clearance for Applicant. The SOR recommended referral to an administrative judge to determine whether a clearance should be granted, continued, denied, or revoked.

Applicant received the SOR on April 10, 2012. In an unsworn declaration, dated May 23, 2012,² Applicant responded to the SOR allegations and elected to have his case decided on the written record in lieu of a hearing. A complete copy of the Government's file of relevant material (FORM) was provided to Applicant on November 1, 2012, and he was afforded an opportunity, within a period of 30 days after receipt of the FORM, to file objections and submit material in refutation, extenuation, or mitigation. Applicant received the FORM on November 7, 2012. He timely submitted a response to which there was no objection. The case was assigned to me on January 23, 2013.

Findings of Fact

In his Answer to the SOR, Applicant admitted portions of four of the factual allegations (¶¶ 1.b, 2.a., 3.a., and 4.b.) of the SOR. Applicant's admissions are incorporated herein as findings of fact. He denied the remaining allegations or portions thereof. After a complete and thorough review of the evidence in the record, and upon due consideration of same, I make the following additional findings of fact:

Applicant is a 56-year-old employee of a defense contractor who, since February 2008, has been serving as a program management consultant. He had previously been a senior consultant with two other employers from July 1996 until November 2007 and from November 2007 until February 2008.³ He has never served in the U.S. military.⁴ He was apparently granted a secret security clearance in 2002, but a subsequent application for a top secret security clearance with another government agency was denied in February 2005.⁵ Applicant appealed that decision, but in December 2008, the denial was upheld.⁶

A 1974 high school graduate, Applicant received a bachelor's degree in an unspecified discipline in May 1978, and a master's degree in an unspecified discipline in May 1987. Applicant was married in 1987.

² Item 4 (Applicant's Answer to the SOR, dated May 23, 2012).

³ Item 5, *supra* note 1, at 14-18.

⁴ Item 5, *supra* note 1, at 20.

⁵ Item 6 (Letter from Senior Adjudication Officer, dated February 24, 2005). A clearance decision was issued against Applicant based on the alleged personal conduct and criminal conduct.

⁶ Item 8 (Affidavit, dated February 19, 2010).

As part of the security clearance processing routinely conducted by another government agency, Applicant was interviewed on December 4, 2003, and again on August 11, 2004. At least one of those sessions took place after or during the administering of a polygraph. It is not known if the initial interview was memorialized in writing. A written record of the final interview was prepared, but only a partial version of it was submitted, having been “redacted to delete extraneous, administrative and/or classified information.” A full text of the original document was offered by the other government agency to the DOD for review by me, but that document was not submitted as part of the FORM.⁷ Applicant objected to the admission and consideration of the contents of the partial version, in part, because he was never accorded the opportunity to validate the information contained in the document.⁸

Sexual Behavior and Criminal Conduct

(SOR ¶¶ 1.a. and 2.a.): The allegation is that from 1996 through 1998, Applicant viewed images and videos of child pornography during three separate “stag weekend” trips. Applicant denied the allegation, in part, challenging the “stag weekend” terminology. The weekends, in a remote location in the woods, were with friends and colleagues of the host and were focused on shooting and fishing. The host of the weekends confirmed Applicant’s characterization and noted that the host alone controlled the guest list, and that Applicant only attended the weekends in 1996 and 1997. He added that he had addressed the allegation against Applicant when the other government agency was investigating the issue, but no one ever approached him to interview him.⁹

As for the portion of the allegation related to viewing child pornography, both Applicant and the host acknowledged that on one of those annual weekends an uninvited guest of an invited guest brought to the cabin some X-rated video tapes which he had rented at a commercial video outlet. Applicant was of the belief that the adult pornography “may have included child pornography.” Finding the videos distasteful, the host did not view them, but Applicant did so.¹⁰

⁷ Item 7 (Memorandum for the Record, dated August 14, 2004, attached to Letter from Office of General Counsel (of another government agency), dated March 14, 2012. The narrative presented in Item 7 is an unsigned version of statements purportedly made by Applicant during his security processing. The cover letter, seemingly addressing Fed. R. Evid. 803 (6), *Records of Regularly Conducted Activity*, stated that it is a true, but redacted, copy “of an original record” maintained by the Office of Security in the regular course of business, made by personnel with knowledge of the act or event recorded to make a record to be maintained. A signed, written, and authenticated statement by Applicant or the interviewer/drafter of the entire statement or record was not included in the Item submitted. Furthermore, while the summary may be a true copy of a portion of the original record, there is no evidence reflecting the accuracy of the original record, or how the “personnel with knowledge of the act or event recorded” obtained such knowledge. As noted, a full text of the original document was offered by the other government agency to the DOD for review by me, but that document was not submitted as part of the FORM. Accordingly, in the absence of the “best evidence,” which was purportedly made following the interview, it is difficult to test the reliability or trustworthiness of the documents submitted.

⁸ Declaration of Applicant, dated November 30, 2012, at 1, attached to Applicant’s Response to the FORM.

⁹ Statement of host, dated May 15, 2012, attached to Item 4, *supra* note 2, as Ex. B.

The partial version of the written record of the 2004 interview conducted by the other government agency tells another story. It covers specifics regarding the ages of children depicted, referring to some as being under 10, between 10 and 12, between 10 and 14, and between 12 and 14. It described the females as “Lolita-like” with small breasts, but there is nothing conclusive regarding the ages of the individuals depicted in the videos. It rambles on, mixing activities at the cabin weekends with activities which purportedly took place in 2002 on a computer. It also includes an opinion that if the police or other authorities had shown up at the cabin, the attendees would have been arrested.

(SOR ¶¶ 1.b. and 2.b.): The allegation is that in about 2002, Applicant viewed images of child pornography on his home computer. Applicant denied the allegation, in part, admitting that he had viewed adult pornography on his home computer, but denying that child pornography was also viewed. He explained that the interviewer of the other government agency asked whether some of the material Applicant viewed “could have been” child pornography, and Applicant replied that it was possible.¹¹ The mere possibility that the images he viewed could have been child pornography, in the absence of other evidence, does not conclusively prove that it was.

The partial version of the written record of the 2004 interview conducted by the other government agency tells another story. In it, Applicant purportedly first admitted and then denied ever deliberately searching for pornography on his home computer. The apparent inconsistencies were not addressed. The version describing such use covers specifics regarding the ages of children depicted, referring to them as being between 10 and 13. It described the females as “Lolita-like”, but there is nothing conclusive regarding the ages of the individuals depicted on the Internet site he visited.

(SOR ¶¶ 1.c. and 2.c.): The allegation is that Applicant viewed images of child pornography in one or more magazines, without any reference to a timeframe. Applicant denied ever viewing child pornography in magazines. He admitted that when he was in his 20’s and working on construction sites, during the years 1978 until 1981, he sometimes purchased magazines depicting adult pornography or viewed the same type of magazines purchased by colleagues.

Once again, the partial version of the written record of the 2004 interview conducted by the other government agency tells two stories. In one part, Applicant discussed the magazines he viewed while working in construction. He stated that the images of the females were of women who were prepubescent, but there is nothing conclusive regarding the ages of the individuals depicted. In the section related to activities in the cabin, Applicant purportedly referred to viewing images of children under 10 in a magazine three or four years prior to the 1996-1998 cabin weekends. Aside from the age guesstimate by Applicant, according to the other government agency, there is nothing conclusive regarding the ages of the individuals depicted.

¹⁰ Item 4, *supra* note 2, at 2; Statement of host, *supra* note 9, at 1.

¹¹ Item 4, *supra* note 2, at 3.

There is no evidence that Applicant was ever disciplined by employers or questioned or charged by police authorities with respect to any of the foregoing allegations.

Use of Information Technology Systems

(SOR ¶ 3.a.): The allegation is that in about 2002, Applicant searched keywords “cock” and “titty” to view pornographic images on his work computer. Applicant denied that he had ever used his office computer to search for pornography. He explained that during his annual ethics and information technology (IT) training he was reminded that there was no expectation of privacy with respect to company computers. Nevertheless, there is no evidence of a rule, procedure, guideline, regulation, or policy from the employer which might prohibit the alleged use. The absence of an expectation of privacy does not equate to the presence of such a rule, policy, etc. Applicant’s attention to detail and following regulations were important, and it is “not at all likely” or actually it was “highly unlikely” that the alleged behavior occurred.¹² He denied ever using his company computer for such purposes, but conceded that he did search such terms and view images of adult pornography on his home computer.¹³ There is no evidence that Applicant’s work computer was ever downloaded and analyzed either by the employer or by government authorities to confirm the allegation. On one occasion, Applicant received an unsolicited e-mail on his work computer which included a pornographic image, but there is no evidence that it contained child pornography or was solicited by Applicant. He noted that the partial version of the written record of the 2004 interview conducted by the other government agency incorrectly reversed his statements about the company and home computers.

Personal Conduct

In addition to the personal conduct issues related to Applicant’s misuse of the IT system at work in about 2002, and the viewing of child pornography during the 1996-1998 “stag weekends” and 2002 on his home computer, as well as the magazine images during the unspecified periods, as set forth in SOR and previously described **(SOR ¶¶ 1.a. through 1.c., and 3.a.)**, the SOR alleged that Applicant falsified material facts during an interview conducted by the other government agency in August 2004 **(SOR ¶ 4.b.)**; that he omitted and concealed information pertaining to the alleged facts set forth in SOR ¶¶ 1.a. through 1.c. when he completed his SF 86 in May 2009 **(SOR ¶ 4.c.)**; and that he falsified material facts during an interview conducted by an investigator from the Office of Personnel Management (OPM) and memorialized in an Affidavit signed by Applicant on February 19, 2010 **(SOR ¶ 4.d.)**.

Based on the contents of the partial version of the written record of the 2004 interview by the other government agency, it was reported that Applicant had stated during two interviews conducted by that other government agency that on various

¹² Item 4, *supra* note 2, at 12.

¹³ Item 4, *supra* note 2, at 3,12.

occasions at least from 1996 until 2002, Applicant had deliberately viewed child pornography, and explained his methods of doing so. Based on the contents of that partial version of the written record, when Applicant subsequently disputed or explained his purported admissions, Department Counsel contends Applicant provided false information regarding the full extent of his viewing of child pornography. By disputing or disavowing the contents of the partial version of the written record of the 2004 interview conducted by the other government agency, according to Department Counsel, he has repeatedly lied about his actions and activities, and he has proven to be unreliable and untrustworthy.

Character References and Work Performance

A former colleague (Applicant's weekend host during the "stag weekends), the leader of a religious-based community service and charitable organization, and the business manager of his church, have all commented favorably about Applicant. They have characterized him as honorable, completely trustworthy, and possessing the utmost integrity.¹⁴ Applicant's performance assessments covering the period from 2008 through 2012 reflect a high quality performer.¹⁵ One comment of significance from a supervisor was noted, suggesting that Applicant "might hone his communication skills to enhance the engagements and exchange of information with team members . . . to mitigate any . . . misinterpretation of any comments during collaborative efforts."¹⁶

Policies

The U.S. Supreme Court has recognized the substantial discretion of the Executive Branch in regulating access to information pertaining to national security emphasizing, "no one has a 'right' to a security clearance."¹⁷ As Commander in Chief, the President has the authority to control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to have access to such information. The President has authorized the Secretary of Defense or his designee to grant an applicant eligibility for access to classified information "only upon a finding that it is clearly consistent with the national interest to do so."¹⁸

When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the AG. In addition to brief introductory explanations for each guideline, the AG list potentially disqualifying conditions and mitigating conditions, which are used in evaluating an applicant's eligibility for access to classified information.

¹⁴ Character References, various dates, attached to Item 4, *supra* note 2, as Ex. B through Ex. D.

¹⁵ Performance Assessments, various dates, attached to Item 4, *supra* note 2, as Ex. E.

¹⁶ Performance Assessment (2012), *supra* note 15, at 2.

¹⁷ *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988).

¹⁸ Exec. Or. 10865, *Safeguarding Classified Information within Industry* § 2 (Feb. 20, 1960), as amended and modified.

An administrative judge need not view the guidelines as inflexible, ironclad rules of law. Instead, acknowledging 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. 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 meaningful decision.

In the decision-making process, facts must be established by "substantial evidence."¹⁹ The Government initially has the burden of producing evidence to establish a potentially disqualifying condition under the Directive, and has the burden of establishing controverted facts alleged in the SOR. Once the Government has produced substantial evidence of a disqualifying condition, under Directive ¶ E3.1.15, the applicant has the burden of persuasion to present evidence in refutation, explanation, extenuation or mitigation, sufficient to overcome the doubts raised by the Government's case. The burden of disproving a mitigating condition never shifts to the Government.²⁰

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 as well. It is because of this special relationship that the Government must be able to repose a high degree of trust and confidence in those individuals to whom it grants access to classified information. Decisions include, by necessity, consideration of the possible risk the applicant may deliberately or inadvertently fail to safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation as to potential, rather than actual, risk of compromise of classified information. Furthermore, "security clearance determinations should err, if they must, on the side of denials."²¹

Clearance decisions must be "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned."²² Thus, nothing in this decision should be construed to suggest that I have based this decision, in whole or in part, on any express or implied determination as to Applicant's allegiance, loyalty, or patriotism. It is merely an indication the Applicant has or has not met the strict guidelines the President and the Secretary of Defense have established for issuing a clearance. In reaching this decision, I have drawn only those conclusions that are

¹⁹ "Substantial evidence [is] such relevant evidence as a reasonable mind might accept as adequate to support a conclusion in light of all contrary evidence in the record." ISCR Case No. 04-11463 at 2 (App. Bd. Aug. 4, 2006) (citing Directive ¶ E3.1.32.1). "Substantial evidence" is "more than a scintilla but less than a preponderance." See *v. Washington Metro. Area Transit Auth.*, 36 F.3d 375, 380 (4th Cir. 1994).

²⁰ See ISCR Case No. 02-31154 at 5 (App. Bd. Sep. 22, 2005).

²¹ *Egan*, 484 U.S. at 531

²² See Exec. Or. 10865 § 7.

reasonable, logical, and based on the evidence contained in the record. Likewise, I have avoided drawing inferences grounded on mere speculation or conjecture.

Analysis

Guideline D, Sexual Behavior

The security concern for Sexual Behavior is set out in AG ¶ 12:

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. No adverse inference concerning the standards in this Guideline may be raised solely on the basis of the sexual orientation of the individual.

The guideline notes several conditions that could raise security concerns. Under AG ¶ 13(a), *sexual behavior of a criminal nature, whether the individual has been prosecuted* is potentially disqualifying. Similarly, under AG ¶ 13(c), *sexual behavior that causes an individual to be vulnerable to coercion, exploitation, or duress* may raise security concerns. In addition, *sexual behavior of a public nature and/or that reflects lack of discretion or judgment* is potentially disqualifying under AG ¶ 13(d). Applicant's alleged history of viewing nude images and pornographic videos of what he believed to be prepubescent children between 1996 and 2002, is documented in the partial version of the written record of the 2004 interview by the other government agency. If true, Applicant's behavior would appear to be of a criminal nature. It reflected a lack of discretion or judgment, and it made him vulnerable to coercion, exploitation, or duress. AG ¶¶ 13(a), 13(c), and 13(d), apply.

The guidelines also include examples of conditions that could mitigate security concerns arising from sexual behavior. Under AG ¶ 14(b), the disqualifying condition may be mitigated where *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*. If *the behavior no longer serves as a basis for coercion, exploitation, or duress*, it is potentially mitigating under AG ¶ 14(c). Similarly, if *the sexual behavior is strictly private, consensual, and discreet*, AG ¶ 14(d) may apply.

AG ¶ 14(b) partially applies. The sole source of the evidence related to Applicant's sexual behavior is himself, as there were no second parties (except for a witness who corroborated Applicant's position regarding the "stag weekend"), identified victims, or arrests. The sexual behavior alleged, if it is to be believed, consisted of three distinctly different episodes: viewing possible child pornography in commercial magazines during the period 1978 until 1981 – over 30 years ago; unexpectedly viewing possible child pornography on one occasion during a "stag weekend" in 1996 or 1997 – over 15 years ago; and viewing images of possible child pornography on a home

computer in about 2002 – 10 years ago. The period since the most recent episode was so long ago, without recurrence, that I conclude that the alleged sexual behavior, if it did occur, is unlikely to recur and does not cast doubt on Applicant’s current reliability, trustworthiness, or good judgment. As noted above, Applicant denied that the images were of children, but did concede that they “could have been of children” since some of the images appeared to be of individuals who were prepubescent or “Lolita-like.” There is nothing conclusive regarding the ages of the individuals depicted.

There is no signed, written, and authenticated statement by Applicant or the interviewer/drafter of the entire statement from the other government agency with respect to the 2003 or 2004 interviews. While the partial version of the written record may be a true copy of that record, there is no evidence reflecting the accuracy of the original record, or how the “personnel with knowledge of the act or event recorded” obtained such knowledge. In the absence of the “best evidence” which was purportedly made following the interview, it is difficult to test the reliability or trustworthiness of the documents submitted, and after considering all of the conflicting evidence, I conclude that the signed unsworn and sworn statements are more reliable than an unsigned redacted summary.

AG ¶ 14(c) applies. Applicant’s wife and his former colleague have been aware of his purported sexual behavior from his past since at least 1996 or 1997, and the Government has been aware of his purported sexual behavior from his past since at least 2003. After those periods of time, with no evidence of further recurrence, that sexual behavior no longer serves as a basis for coercion, exploitation, or duress.

AG ¶ 14(d) does not apply. While Applicant’s unexpected and deliberate viewing of pornographic images and videos that may have included images of prepubescent individuals took place in private and discreet locations – a private cabin and his home – and was not openly broadcast to others, and no criminal action was ever proposed or taken against Applicant for his actions. Prepubescent children – essentially exploited victims – cannot, under the law, consent to such behavior.

Guideline J, Criminal Conduct

The security concern under the guideline for Criminal Conduct is set out in AG ¶ 30:

Criminal activity creates doubt about a person's judgment, reliability, and trustworthiness. By its very nature, it calls into question a person's ability or willingness to comply with laws, rules and regulations.

The guideline notes several conditions that could raise security concerns. Under AG ¶ 31(a), *a single serious crime or multiple lesser offenses* is potentially disqualifying. Similarly, under AG ¶ 31(c), if there is *an allegation or admission of criminal conduct, regardless of whether the person was formally charged, formally prosecuted or convicted*, security concerns may be raised. As noted above, during a “stag weekend” in either 1996 or 1997, Applicant inadvertently viewed what may have been child

pornography; in 2002 he may have viewed child pornography on his home computer; and during an unspecified period, identified by Applicant as occurring during 1978 until 1981, he may have viewed child pornography in commercially available magazines. While Applicant may have estimated the ages of the individuals viewed, the mere possibility that those images were of prepubescent children, in the absence of other evidence, does not conclusively prove that they were. Nevertheless, considering the mere possibility that the individuals were prepubescent children, as conceded by Applicant, further discussion is necessary. Accordingly, AG ¶¶ 31(a) and 31(d) have been established.

The guideline also includes examples of conditions that could mitigate security concerns arising from criminal conduct. Under AG ¶ 32(a), the disqualifying condition may be mitigated where *so much time has elapsed since the criminal behavior happened, or it happened under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment.* Likewise, if there is *evidence that the person did not commit the offense,* ¶ 32(c) may apply. Similarly, AG ¶ 32(d) may apply where *there is evidence of successful rehabilitation: including but not limited to the passage of time without recurrence of criminal activity, remorse or restitution, job training or higher education, good employment record, or constructive community involvement.*

AG ¶¶ 32(a), 32(c), and 32(d) apply. As noted above, the alleged criminal behavior consisted of three distinctly different episodes: viewing possible child pornography in commercial magazines during the period 1978 until 1981 – over 30 years ago; unexpectedly viewing possible child pornography on one occasion during a “stag weekend” in 1996 or 1997 – over 15 years ago; and viewing images of possible child pornography on a home computer in about 2002 – 10 years ago. There has been no recurrence of those alleged criminal activities in the past 30, 15, or 10 years. Applicant has maintained a good employment record and has an excellent reputation in the community. It is unlikely that such criminal behavior will recur, and it no longer casts doubt on his reliability, trustworthiness, or good judgment.

Guideline M, Information Technology

The security concern under the guideline for Use of Information Technology Systems is set out in AG ¶ 39:

Noncompliance 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 Systems include all related computer hardware, software, firmware, and data used for the communication, transmission, processing, manipulation, storage, or protection of information.

The guideline notes conditions that could raise security concerns. Under AG ¶ 40(e), security concerns may be raised by: *the unauthorized use of a government or other information technology system*. In about 2002, Applicant purportedly searched keywords “cock” and “titty” to view pornographic images on his work computer. He denied the allegation as not likely, and asserted the search took place on his home computer. While there may be no expectation of privacy with respect to Applicant’s employer’s company computers, there is no evidence of a rule, procedure, guideline, regulation, or policy from the employer which might prohibit the alleged use. Nevertheless, considering the mere possibility that there were prohibitions in place, further discussion is necessary. Accordingly, AG ¶ 40(e) has been established.

The guideline also includes examples of conditions that could mitigate such security concerns. Under AG ¶ 41(a), the disqualifying condition may be mitigated where *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*. The alleged activity took place on one occasion in about 2002, and there is no evidence to suggest that it happened more than once or that it took place more recently. Assuming the accuracy of the allegation, the passing of over ten years without recurrence is sufficient to conclude that it is unlikely to recur, and it does not cast doubt on Applicant’s reliability, trustworthiness, or good judgment. AG ¶ 41(a) applies.

Guideline E, Personal Conduct

The security concern for Personal Conduct is set out in AG ¶ 15:

Conduct involving questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations can raise questions about an individual's reliability, trustworthiness and ability to protect classified information. Of special interest is any failure to provide truthful and candid answers during the security clearance process or any other failure to cooperate with the security clearance process.

The guideline notes conditions that could raise security concerns. Under AG ¶ 16(b), security concerns may be raised by: *deliberately providing false or misleading information concerning relevant facts to an employer, investigator, security official, competent medical authority, or other official government representative*.

Similarly, security concerns may be raised under AG ¶ 16(c) if there is:

credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any other single guideline, but which, when considered as a whole, supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the person may not properly safeguard protected information.

Also, it is potentially disqualifying under AG ¶ 16(e) when there is:

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. . . .

The alleged criminal behavior consisted of viewing possible child pornography in commercial magazines over 30 years ago; unexpectedly viewing possible child pornography on one occasion over 15 years ago; and viewing images of possible child pornography on a home computer about 10 years ago. There has been no recurrence of those alleged criminal activities. The other alleged personal conduct issues relate to Applicant's responses to questions in his SF 86 in 2009 – over three years ago; and his comments in an affidavit in 2010 – nearly three years ago. There is insufficient evidence to conclude that Applicant deliberately provided false or misleading information concerning the issue of child pornography or to his use of his work computer. To the contrary, Applicant has been consistent in his rendition of the facts. Disagreeing with summarized unverified information in the record does not establish that he deliberately lied. A summary or partial version of the written record of the 2004 interview prepared by an unknown person does not have the same indicia of reliability as an affidavit. Accordingly, AG ¶ 16(e) has been established, but AG ¶¶ 16(b) and 16(d) have not.

The guideline also includes examples of conditions that could mitigate security concerns arising from personal conduct. AG ¶ 17(c) may apply if *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.*

Similarly, AG ¶ 17(d) may apply if:

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 caused untrustworthy, unreliable, or other inappropriate behavior, and such behavior is unlikely to recur.

Also, if *the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress*, AG ¶ 17(e) may apply. In addition, AG ¶ 17(f) may apply if *the information was unsubstantiated or from a source of questionable reliability.*

As to Applicant's alleged self-reported misuse of his employer's IT system in 2002, as noted above, there were no adverse consequences of his actions, and there is no evidence that Applicant misused employer IT systems since the last incident.

The Government concluded that since Applicant's statements disagree with the information submitted by the other government agency, Applicant must now be lying. The summary or partial version of the written record of the 2004 interview prepared by

an unknown person, without any indication that the contents were verified as accurate by Applicant or the drafter of the summary, when the original transcript of the interview – the best evidence of what was actually said – is still available, is essentially unsubstantiated, and does not have the same indicia of reliability as an affidavit. An unsubstantiated or unverified summary may contain inaccuracies such as those stated by Applicant. Slight variations of words or responses, as well as the selected portions of an entire document, may convey entirely different impressions and may lead to substantial misinterpretation. Applicant has consistently refuted the contents of the summary of an existing file submitted by the other government agency. To the extent that the alleged sexual behavior of between 12 and 30 years ago might have taken place, Applicant has taken positive steps to both alleviate the circumstances or factors that may have caused his alleged untrustworthy, unreliable, or other inappropriate behavior, and reduce or eliminate his vulnerability to exploitation, and such behavior is unlikely to recur. AG ¶¶ 17(c), 17(d), 17(e), and 17(f) apply.

Whole-Person Concept

Under the whole-person concept, the administrative judge must evaluate an applicant's eligibility for a security clearance by considering the totality of the applicant's conduct and all the circumstances. The 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.

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. Moreover, I have evaluated the various aspects of this case in light of the totality of the record evidence and have not merely performed a piecemeal analysis.²³

There is some evidence against mitigating Applicant's sexual behavior, criminal behavior, use of information technology systems, and personal conduct. Applicant allegedly viewed images of prepubescent children in videos, in magazines, and on his home computer, as well as misused his employer's IT system in 2002. He denied most of the allegations, but there is some information that he may have done so with some frequency. That information is not entirely reliable. Applicant acknowledged that he routinely viewed adult pornography.

²³ See *U.S. v. Bottone*, 365 F.2d 389, 392 (2d Cir. 1966); See also ISCR Case No. 03-22861 at 2-3 (App. Bd. Jun. 2, 2006).

The mitigating evidence under the whole-person concept is more substantial. Applicant's alleged sexual behavior, criminal behavior, use of information technology systems, and personal conduct occurred between 10 and 30 years ago, if it is to be believed that it occurred, and there is no evidence of subsequent conduct of a similar nature. There is no evidence of a personality disorder. Applicant has a good reputation for integrity and trustworthiness, but, according to his supervisor, also an apparent shortcoming in communication skills leading to possible misinterpretation of his comments. No disciplinary or criminal action was ever proposed or taken against him for his alleged actions. The alleged behavior is unlikely to recur. Under the evidence presented, I have no questions about Applicant's reliability, trustworthiness, and ability to protect classified information. See AG ¶ 2(a)(1) through AG ¶ 2(a)(9).

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:	FOR APPLICANT
Subparagraph 1.a:	For Applicant
Subparagraph 1.b:	For Applicant
Subparagraph 1.c:	For Applicant
Paragraph 2, Guideline J:	FOR APPLICANT
Subparagraph 2.a:	For Applicant
Paragraph 3, Guideline M:	FOR APPLICANT
Subparagraph 3.a:	For Applicant
Paragraph 4, Guideline E:	FOR APPLICANT
Subparagraph 4.a:	For Applicant
Subparagraph 4.b:	For Applicant
Subparagraph 4.c:	For Applicant
Subparagraph 4.d:	For Applicant

Conclusion

In light of all of the circumstances presented by the record in this case, it is clearly consistent with the national interest to grant Applicant eligibility for a security clearance. Eligibility for access to classified information is granted.

ROBERT ROBINSON GALES
Administrative Judge