



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



In the matter of:)	
)	
REDACTED)	ISCR Case No. 11-09770
)	
Applicant for Security Clearance)	

Appearances

For Government: David Hayes, Esq., Department Counsel
For Applicant: Bradley P. Moss, Esq.

09/30/2013

Decision

MENDEZ, Francisco, Administrative Judge:

Applicant did not mitigate the personal conduct, sexual behavior, and misuse of information technology security concerns. Over the course of six years, from 2003 to 2009, he actively searched for, received, and viewed child pornography. He also hacked into the e-mail, internet, and computer accounts of others looking for images to gratify his deviant sexual interests. Applicant's past conduct continues to cast doubt on his current reliability, trustworthiness, and good judgment. Clearance is denied.

Statement of the Case

On February 28, 2013, the Department of Defense (DoD), in accordance with DoD Directive 5220.6, as amended (Directive), issued Applicant a Statement of Reasons (SOR), alleging security concerns under Guideline M (Use of Information Technology Systems), Guideline D (Sexual Behavior), and Guideline E (Personal Conduct). On March 13, 2013, Applicant answered the SOR and requested a hearing.

On May 9, 2013, I was assigned Applicant's case and after coordinating with the parties, scheduled the hearing for June 3, 2013. Applicant requested a continuance due

to the unavailability of his expert witness. I granted the continuance request, which was unopposed. The hearing was rescheduled for June 27, 2013.

At hearing, Government Exhibits (Gx.) 1 and 2 and Applicant's Exhibits (Ax.) 1 through 12 were admitted into evidence without objection.¹ Applicant called several witnesses and testified. He requested additional time post-hearing to submit a declaration from an additional character reference. I granted his request and he timely submitted Ax. 13, which was admitted without objection. The hearing transcript (Tr.) was received on July 8, 2013, and the record closed on July 19, 2013.

Findings of Fact

Applicant, 30, is single and has no children. He graduated from a prestigious university with a bachelor's degree in information technology (IT) in 2005. He then worked in the People's Republic of China (PRC) with a religious organization, as a missionary and the organization's regional IT director. He returned to the United States in 2007, and started working as a defense contractor. He has been with his current employer since 2008. He has been entrusted with classified information in the past, and testified that he has never mishandled or compromised such information. His employer and past supervisor praise his work and recommend him for a security clearance. (Tr. at 54-79, 152-158; Gx. 1 – 2; Ax. 3 – 4)

In 2008, Applicant was granted a security clearance. In 2009, he was interviewed by another government agency (AGA) in connection with his application to work on a classified project requiring access to Sensitive Compartmented Information (SCI). He submitted to an interview and polygraph by the AGA in June 2009. Applicant was unable to pass the polygraph portion of the interview and was deeply troubled by one particular question asked by the AGA agent, namely, "have you ever been involved in any serious crime?" (Gx. 2 at 108, Tr. at 163) Applicant submitted to a second polygraph-assisted interview five months later in November 2009. During the course of the two interviews, Applicant revealed that he intentionally searched for, viewed, and masturbated to child pornography from 2003 to 2009. Applicant also revealed that, between 2004 and 2009, he violated the trust of several friends and co-workers by accessing their e-mail, internet, and computer accounts without permission. Based on Applicant's admissions, his request for SCI access was denied and his security clearance was later suspended. (Gx. 2 at 91-107, 112-113, 127-128; Tr. at 164-165)

During the two AGA interviews, Applicant told the agent he knew that the images he viewed were of minor children based on their lack of physical development and other distinguishing characteristics (i.e., lack of pubic hair, breast development, and facial features). He "acknowledged that the girls under the age of 18 were in sexually provocative positions and were exposing their genitals." (Gx. 2 at 106) He searched for child pornography by using the following search terms: "preteens, thirteen year old girls, fourteen year old girls, fifteen year old girls, and sixteen year old girls." (Gx. 2 at

¹ Gx. 2 is 249 pages long. I have added page numbers on the upper right hand corner for ease of reference.

95) He also told the AGA agent that he searched for images of child pornography on a preteen newsgroup, using the search term “teen.” (Gx. 2 at 94) In his appeal of the SCI denial, Applicant stated that “[t]he information I provided during the polygraph interviews was accurate and true.” He also admitted that, from age 20 to 26, he employed “search terms targeting women under 18.” (Gx. 2 at 115)

At hearing, Applicant claimed to have no recollection of any of the images of child pornography he viewed, except for one involving a naked child before a black background. He testified that he cannot recall whether any of the images of child pornography depicted sexually-explicit acts. However, he continues to acknowledge the images he viewed from 2003 to 2009 constituted child pornography and that child pornography is illegal. (Tr. at 172-177, 266-267).

Applicant testified that he did not know what he was doing when he searched for, viewed, and masturbated to images of child pornography. (Tr. at 170-178) He testified that “I really was not thinking. . . . I was clicking through different categories of things, just looking to see what was there, what different pornography I discovered. My mind was not engaged in thinking about what was right and wrong, what the consequences of my actions were.” (Tr. at 171) Applicant went on to state that when he used specific search terms, such as preteen, he simply reverted back to his old habits as a teenager, without realizing that his actions were wrong and illegal. (Tr. at 171-174, 177)²

Applicant claims that he has not searched for, received, possessed, or viewed child pornography since the June 2009 AGA interview. He also claims that he is not attracted to minor girls and has no desire to view child pornography. (Tr. at 170-178) However, as of the second AGA interview in November 2009, Applicant was still searching the internet for pornography involving young women and was employing the search term “teen.” (Gx. 2 at 94)

As for accessing others’ computer accounts without their permission, Applicant revealed during the AGA interviews that, starting in 2004, he broke into the internet accounts of three female friends who had turned down his romantic advances. He gained access to all three women’s accounts after they provided him their passwords to fix their computers. Applicant went to college with one of the women. He accessed her Facebook account using her password and would view her photographs, as well as those of her friends. In some of the photographs the females were in bathing suits and appeared to be minors. He would masturbate to these photographs. He continued to access this individual’s Facebook account for the next five years. He stopped shortly before his second AGA interview in 2009. Applicant testified that he still recalls the password to the Facebook account, but claims to have not accessed it since 2009.

Applicant met the other two women whose internet accounts he improperly accessed while working in the PRC. He accessed their e-mail accounts hoping to find

² See also Ax. 1 at 3; Tr. at 97-98 (Expert witness opines that Applicant committed the acts at issue in a “dissociative/compulsive” manner and, while in this purported state, Applicant was in a “world of fantasy where rules and laws and ages are all outside and you are in another world.”).

images of them or others to satisfy his sexual desires. He continued accessing their e-mail accounts after returning to the United States. He last accessed their e-mail accounts without permission in 2008. (Tr. at 189-199, 213-226, 270-271; Gx. 1 at 56; Gx. 2 at 94-95, 105, 110) Applicant claims he has not informed the three women whose trust and privacy he violated because he does not want to cause them any further harm. (Tr. at 199)

At hearing, Applicant admitted to improperly accessing other individuals' computer and e-mail accounts while serving as the regional IT director of the religious organization. He did so looking for images to satisfy his sexual desires. In 2007, a co-worker, who was also a friend, asked Applicant for some help transferring data from an old computer to a new one. While working on the computer, Applicant testified that he "stumbled across" several images of a "scantily clad" woman. (Tr. at 230-231) He copied the images to another file and later masturbated to the images. (Tr. at 197-199, 230-233) Applicant eventually admitted that the scantily clad woman in the images was his colleague's wife. (Tr. at 271-272) Applicant still sees his former colleague's wife from time-to-time, but has not told either of them what he did. (Tr. at 199, 233, 272)

Also, in his role as regional IT director, Applicant gained access to the computer passwords of several individuals. In approximately mid-2008, he used the passwords to access five to ten different computer accounts, looking for images to gratify his sexual desires. He claims to have told the current IT director of his misconduct. Although a number of individuals from the religious organization submitted letters on his behalf, none state that he admitted to abusing his position with the organization to hack into other individuals' computer accounts. (Tr. at 226-230, Gx. 2 at 56)³

Applicant posits that he can once again be entrusted with classified information. He notes that over the past four years he has had access to other individual's computer accounts and has not inappropriately accessed anyone's accounts, to include the accounts of women who have rejected his romantic advances. (Tr. at 201-203) Also, he has received professional counseling through his church. His counselor submitted a letter noting that Applicant continues to use appropriate coping techniques and mechanisms to handle stress. (Ax. 8)

Applicant installed a software program on his computer that presumably provides an extra layer of protection. The software monitors his internet search activity, detects if he goes to any sexually-explicit sites, and informs his "accountability partner" of his internet activity. However, Applicant admitted at hearing that he signed up for this software program prior to 2005, and it did not prevent his child pornography activity. (Tr. at 244 – 251; Gx. 2 at 118; Ax. 6)

³ See, e.g., Ax. 2 (senior staffer for the religious organization writes that he was provided the SOR, but nowhere states that he is aware the hacking allegations involve Applicant's abuse of his position with the organization); Ax. 13 (pastor notes that Applicant admitted his "online pornography" addiction, but nothing about the improper access of other individuals' computer accounts).

Applicant told a number of friends, co-workers, and family members of his misconduct. A number of these individuals submitted letters and testified about his trustworthiness, reliability, and law abidingness. They all state that Applicant's past conduct is uncharacteristic behavior, and recommend him for a security clearance. (Tr. at 19-53, Ax. 2, 5 – 7, 9 – 13)

Applicant called Dr. X, a clinical psychologist, as an expert witness. Dr. X evaluated the Applicant about a month before the hearing and prepared a report that was admitted as Ax. 1. According to Dr. X, Applicant's obesity as a teenager impacted his self-esteem and caused a significant delay in his psycho-social-sexual development and maturation. (Ax. 1 at 2 – 3; Tr. at 103-104) Applicant turned to pornography as a teenager and his fixation with young girls continued into adulthood. (Ax. 1 at 3) After a period of time, Applicant started to recognize the inappropriateness of his behavior and took steps to curtail it, but he would relapse and constantly struggled with his "behavioral addiction." (Ax. 1 at 4) Dr. X opined in his report that Applicant's behavior did not meet the criteria for pedophilia. He diagnosed Applicant with anxiety disorder. (Ax. 1 at 5; Tr. at 109-110) He further opined that it was "unlikely that [Applicant] would ever return to these behaviors in the future." (Ax. 1 at 5)

At hearing, Dr. X further elaborated on the opinions contained in his report. He maintained that Applicant did not currently meet the criteria for pedophilia. (Tr. at 149) However, he stated that there are some reliable diagnostic tests used by experts to determine if an individual "has traits consistent with pedophilia," but he did not employ any such test in his evaluation of Applicant. (139-140, 147) Dr. X acknowledged that Applicant's conduct in seeking out both adult and child pornography was consistent with a non-exclusionary type of pedophilia. (Tr. at 105) He also testified that Applicant never told him of using the search term "preteen" and, if he had, Dr. X's diagnosis would likely have been different, as Applicant's conduct "would be closer to the diagnosis of pedophilic behavior." (Tr. at 120, 138, 146-147) Applicant claims that he told Dr. X of using the preteen search term. (Tr. at 207)

Dr. X also clarified his opinion that it was "unlikely" Applicant would engage in similar conduct in the future. He testified that he could not completely rule out the possibility that Applicant would relapse, and listed a number of risk factors, to wit: isolation, family crisis, job lost, weight gain, and "other things" that could affect Applicant's sense of self. Notwithstanding this observation, Dr. X continued to assess the risk of relapse as relatively low and quantified the risk at one to five percent. (Tr. at 111-113, 127, 136)

Dr. X concluded his report and testimony by recommending that Applicant seek further treatment to resolve the underlying issues that led him to engage in the inappropriate behavior. Notably, Dr. X recommended that Applicant pursue individual psychotherapy and mixed gender group therapy (Ax. 1 at 6; Tr. at 124-125, 136). Applicant testified that he intended to "adhere" to Dr. X's recommendation. (Tr. at 209) As of the close of the record, no evidence was presented that Applicant complied with Dr. X's treatment advice.

Policies

“[N]o one has a ‘right’ to a security clearance.” *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988). Individual applicants are only eligible for access to classified information “only upon a finding that it is clearly consistent with the national interest” to authorize such access. Executive Order (E.O.) 10865, *Safeguarding Classified Information within Industry*, § 2 (Feb. 20, 1960), as amended.

When evaluating an applicant’s eligibility, an administrative judge must consider the adjudicative guidelines (AG). In addition to brief introductory explanations, the guidelines list potentially disqualifying and mitigating conditions. The guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, an administrative judge applies the guidelines in a common sense manner, considering all available and reliable information, in arriving at a fair and impartial decision.

The Government must present evidence to establish controverted facts alleged in the SOR. Directive ¶ E3.1.14. On the other hand, an applicant is responsible for presenting “witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by the applicant or proven by Department Counsel.” Directive ¶ E3.1.15. An applicant has the ultimate burden of persuasion to establish their eligibility.

In resolving the ultimate question regarding an applicant’s eligibility, an administrative judge must resolve “[a]ny doubt concerning personnel being considered for access to classified information . . . in favor of national security.” AG ¶ 2(b). Moreover, “security clearance determinations should err, if they must, on the side of denials.” *Egan*, 484 U.S. at 531.

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. 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 an applicant may deliberately or inadvertently fail to safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation of potential, rather than actual, risk of compromise of classified information.⁴

Clearance decisions must be made “in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned.” E.O. 10865 § 7. Thus, a decision to deny a security clearance amounts to a finding that an applicant, at the time the decision was rendered, did not meet the strict guidelines established for determining eligibility for access to classified information.

⁴ See generally *Kaplan v. Conyers, et al.*, 2013 U.S. App. LEXIS 17278 at ** 23-24, 40-51 (Fed. Cir. Aug. 20, 2013) (federal courts will generally defer to the predictive judgments made by executive branch officials responsible for determining the eligibility of an applicant for a security clearance).

Analysis

Guideline E, Personal Conduct

The personal conduct security concern is set forth at 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.

Applicant's conduct from 2003 to 2009 in searching for and viewing child pornography and improperly accessing other individuals' computer accounts raises the Guideline E concern. Applicant's conduct also establishes 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 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, or (2) while in another country, engaging in any activity that is illegal in that country or that is legal in that country but illegal in the United States and may serve as a basis for exploitation or pressure by the foreign security or intelligence service or other group.

The evidence presented by Applicant also raised the potential applicability of the following mitigating conditions under AG ¶ 17:

(c) the offense is so minor, or so much time has passed, or the behavior is so infrequent, or it happened under such unique circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment;

(d) the individual has acknowledged the behavior and obtained counseling to change the behavior or taken other positive steps to alleviate the stressors, circumstances, or other 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.

Applicant claims that he has not repeated any of the conduct at issue since 2009 and has taken a number of steps to avoid engaging in such conduct in the future. However, I am not convinced that similar conduct will not recur and for the reasons set forth below do not find that ¶¶ 17(c), 17(d), and 17(e) fully apply.

First, Applicant only stopped engaging in the conduct at issue after being caught with the assistance of two polygraph-assisted interviews. Even after the initial AGA interview, Applicant continued accessing the Facebook account of a woman who rejected his advances in college. He hacked into her account looking for images to gratify his deviant sexual desires. Also, between his first and second AGA interviews, Applicant searched the internet for pornography by using the search term “teen” – a search term he had used in the past to find child pornography.⁵ Applicant’s inability to recognize the wrongfulness of his conduct even after being confronted by the AGA and the fact he only stopped engaging in such conduct after the second AGA interview, calls into question his overall judgment and severely undercuts the mitigating value of the passage of time.⁶

Second, Applicant did not take responsibility for his conduct. At hearing, Applicant explained his conduct by claiming that he was not thinking and could not appreciate the consequences of his actions or even right from wrong. However, the record evidence is clear that over the course of six years, Applicant deliberately and repeatedly scoured the internet for images of child pornography to gratify his deviant sexual interest. He did not simply revert back to his teenage years without thinking, as he testified. Applicant, who has an IT degree and was working in the IT field at the time, deliberately used search terms that he knew from past experience would retrieve images of child pornography. His attempts now to minimize his behavior undercuts the favorable evidence of rehabilitation and raises serious concerns that he may engage in similar conduct in the future.

Third, Applicant also tried to minimize the seriousness of his illegal conduct. At hearing, he claimed to have practically no memory of any of the images he viewed and the only image he now claims to remember can, at best, be described as child erotica.⁷ I found Applicant’s self-serving testimony not credible and misleading. He previously told the AGA that the images he viewed depicted minors with their genitalia exposed and in

⁵ Applicant’s assertion to the AGA agent that he believed using the search term “teen” would only result in finding legal pornography is incredulous considering his background and past experience.

⁶ ISCR Case No. 09-03370 at 4 (App. Bd. Sep. 7, 2011).

⁷ *Cf., United States v. Anderson*, 2010 CCA LEXIS 328, * 2 (Army Ct. Crim. App. Sep. 10, 2012), quoting from and citing to *United States v. Vosburgh*, 602 F.3d 512, 520 (3d Cir. 2010) (defining child erotica as “material that depicts ‘young girls [or boys] as sexual objects or in a sexually suggestive way,’ but is not ‘sufficiently lascivious to meet the legal definition of sexually explicit conduct’ under 18 U.S.C. § 2256” or otherwise criminal).

sexually-provocative poses. Months after he made these inculpatory statements to the AGA, Applicant confirmed the accuracy of the statements. Applicant's attempt now to backtrack from these statements leads me to conclude that he is not fully rehabilitated and calls into question his current trustworthiness and reliability.⁸

Fourth, in assessing the potential that Applicant will engage in similar conduct in the future, I considered the expert's testimony regarding the potential for relapse and the likely risk factors for such relapse. Of particular note, many of the risk factors listed by the expert are common, everyday stressors that no one individual is able to completely avoid. Although Applicant recently handled a negative experience, specifically, rejection by a romantic interest, without relapsing, I gave such evidence little weight because he was pending review of his security clearance and understood any further misconduct would negatively impact his chances to regain his eligibility. As for the expert's assessment that the probability of relapse is relatively low, even if I were to credit such assessment, such a risk is still far too high when it comes to safeguarding this nation's secrets. More importantly, the expert's assessment appears deeply flawed due to Applicant's minimization of his prior conduct.

Fifth, Applicant has not informed any of the individuals whose trust and privacy he violated that he hacked into their e-mail, internet, and computer accounts. His failure to reveal this information to his victims leaves him vulnerable to duress and undue influence.⁹ Applicant's assertion that he has not informed these individuals because he does not wish to bring them further harm was not credible. By not revealing his misconduct, he continues to have the ability to access the Facebook account of a woman who rejected his romantic advances in college. In addition, Applicant engaged in some of this conduct while residing in the PRC. He continued to hack into the e-mail accounts of PRC residents after returning to the United States and being granted a security clearance. He engaged in this activity without considering the possibility that it could subject him to duress or exploitation at the hands of a hostile foreign country.¹⁰

Accordingly, I find that Applicant failed to meet his burden of persuasion to mitigate the personal conduct security concerns. His past conduct continues to call into question his reliability, trustworthiness, and good judgment.

⁸ See ISCR Case No. 11-02334 at 4 (App. Bd. May 15, 2013) (Notwithstanding the fact that the security significant conduct occurred 20 years in the past, applicant's "false and/or minimizing statements provide a reasonable basis for the Judge to have concluded that Applicant had not demonstrated a level of rehabilitation commensurate with the requirements of the Directive.") See *also* ISCR Case No. 11-13644 (App. Bd. Aug. 15, 2013) (applicant's attempts to minimize his conduct and claims of not recalling prior inculpatory statements provided adequate basis for denial).

⁹ See *generally* ISCR Case No. 11-05685 (App. Bd. Jul. 12, 2013) (applicant was left vulnerable to coercion because he did not tell his family members about the security significant conduct).

¹⁰ See *generally* ISCR Case No. 12-00058 (App. Bd. Apr. 9, 2013) (detailing potential security concerns involving the PRC).

Guideline D, Sexual Behavior

The security concern for sexual behavior is addressed at AG ¶ 12:

Sexual behavior that involves a criminal offense, indicates a personality or emotional disorder, reflects lack of judgment or discretion, or which can 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.

Applicant's deviant sexual behavior from 2003 to 2009 raises this concern and establishes all four disqualifying conditions under AG ¶ 13:

- (a) sexual behavior of a criminal nature, whether or not the individual has been prosecuted;
- (b) a pattern of compulsive, self-destructive, or high-risk sexual behavior that the person is unable to stop or that may be symptomatic of a personality disorder;
- (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.

None of the mitigating conditions listed at AG ¶ 14 apply for the reasons noted under the Guideline E analysis. I also note the following additional matter. The expert witness testified that if Applicant had informed him of using the preteen search term, his diagnosis may have been different and possibly closer to pedophilia, a far more serious diagnosis and one more consistent with the record evidence. I did not find Applicant's claim that he told the expert of using the preteen search term credible. Applicant's failure to inform the expert of this significant aspect of the case is consistent with his attempts at hearing to minimize his sexually-deviant conduct. Applicant's conscious decision not to provide this critical information left the expert's opinion regarding the low likelihood of recurrence highly suspect. Furthermore, Applicant did not submit evidence of complying with the expert's treatment advice, which the expert specifically noted was necessary to avoid a relapse. In conclusion, Applicant's past sexual behavior continues to cast doubt on his current eligibility.

Guideline M, Use of Information Technology Systems

AG ¶ 39 articulates the security concern relating to misuse of IT systems:

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, and protection of information.

At first blush, the Guideline M concern does not appear to be applicable. The guideline appears to only address instances where an individual violates specific rules and regulations regarding the proper use of government or a private company's IT systems. However, reading the guideline in such a narrow fashion would be inconsistent with the overall purpose of the Directive, which is to ensure that only those who demonstrate a consistent track record of reliability, trustworthiness, and good judgment are granted access to classified information.

In this case, over the course of five years, Applicant repeatedly breached the trust placed in him by his friends, co-workers, and his former employer by improperly accessing e-mail, internet, and computer accounts. Although the Government did not submit or allege the violation of any specific rule or regulation, Applicant's conduct in hacking into other individual's private internet accounts, at a minimum, violated the policies that the providers of internet services, such as Facebook and e-mail service providers, have for the protection of their users' privacy and information. Furthermore, Applicant clearly abused his position with the religious organization, when he improperly accessed his co-worker's computer accounts looking for images to gratify his sexual desires. He manipulated his former colleague's computer account by transferring and then saving to another file the images of his former colleague's wife. Applicant's testimony that he merely "stumbled across" these images was clearly disingenuous. This record evidence establishes the following disqualifying conditions under AG ¶ 40:

- (a) illegal or unauthorized entry into any information technology system or component thereof; and
- (b) illegal or unauthorized modification, destruction, manipulation or denial of access to information, software, firmware, or hardware in an information technology system.

After thoroughly reviewing all the mitigating conditions listed at AG 41, I find that none apply for the same reasons noted in my Guideline E analysis. Applicant's past misuse of IT systems continues to raise a concern about his current eligibility.

Whole-Person Concept

Under the whole-person concept, an administrative judge must evaluate an applicant's eligibility for a security clearance by considering the totality of an applicant's conduct and all the relevant circumstances. An administrative judge should consider the nine factors listed at AG ¶ 2(a).¹¹ I specifically considered Applicant's work performance, community service, character references, and the steps he has taken to overcome his past behavior. However, the seriousness, length of time, and overall breadth of Applicant's past conduct, as well as his lack of sincerity and minimization of his behavior, leaves me *significant* doubts about his eligibility for a security clearance.

Formal Findings

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

Paragraph 1, Guideline M (Use of IT Systems):	AGAINST APPLICANT
Subparagraphs 1.a – 1.e:	Against Applicant
Paragraph 2, Guideline D (Sexual Behavior):	AGAINST APPLICANT
Subparagraphs 2.a – 2.d:	Against Applicant
Paragraph 3, Guideline E (Personal Conduct):	AGAINST APPLICANT
Subparagraph 3.a:	Against Applicant

Conclusion

In light of the record evidence and for the foregoing reasons, it is not clearly consistent with the national interest to grant Applicant access to classified information. Applicant's request for a security clearance is denied.

Francisco Mendez
Administrative Judge

¹¹ The non-exhaustive list of adjudicative factors are: (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.