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

| | | |
|---|---|---|
| In the matter of: | ) | |
| | ) | |
| | ) | ISCR Case No. 10-04796 |
| | ) | |
| Applicant for Security Clearance | ) | |

## Appearances

For Government: Julie R. Mendez, Esquire, Department Counsel

For Applicant: Mark S. Zaid, Esquire

02/29/2012

## Decision

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

Based on a review of the pleadings, testimony, and exhibits, I conclude that Applicant has not mitigated the security concerns raised under the guidelines for use of information technology systems and personal conduct. Accordingly, his application for a security clearance is denied.

## Statement of the Case

On February 8, 2011, the Defense Office of Hearings and Appeals (DOHA) issued to Applicant a Statement of Reasons (SOR) that detailed security concerns addressed in the Directive under Guideline M (use of information technology systems) and Guideline E (personal conduct) of the Adjudicative Guidelines (AG). The action was taken under Executive Order (EO) 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the adjudicative guidelines (AG) implemented by the Department of Defense on September 1, 2006.

In his March 23, 2011 Answer to the SOR, Applicant requested a hearing before an administrative judge. Department Counsel was prepared to proceed on August 8, 2011, and the case was assigned to me on September 16, 2011. DOHA issued a Notice of Hearing on September 23, 2011, and I convened the hearing as scheduled on October 18, 2011. Department Counsel offered three exhibits, marked as Government Exhibits (GE) 1 through 3, which were admitted into evidence without objection. Applicant testified, presented testimony of two witnesses, and offered 12 exhibits, marked as Applicant Exhibits (AE) A through L, which I admitted into evidence without objection. DOHA received the transcript (Tr.) on October 25, 2011.

## Procedural Matters

By memorandum dated October 14, 2011, Department Counsel amended the SOR before the hearing to add the following new allegations under Guideline M. Applicant denied the new allegations at subparagraphs 1.d through 1.f, and 1.h. He admitted allegation 1.g.

> 1.d. You improperly attempted to hack into your [company A] DoD-contract computer from your home computer.[1]
>
> 1.e. You improperly hacked into Department of Defense computers.
>
> 1.f. While working at [DoD location], sometime between 2001 and 2003, you accessed and surfed the Internet through other users' accounts, without their knowledge or authorization.
>
> 1.g. From about 1995 through 2007, you illegally downloaded at least $200,000 worth of software, music, and movies.
>
> 1.h. As of March 2008, you knowingly viewed images that you characterized as containing underage pornography. Of your pornography viewing, ten percent of the images were of girls that you believed to be under the age of 15.

Department Counsel also struck allegation 2.b under Guideline E, and replaced it with the following allegation, which Applicant denied:

> 2.b. You falsified material facts on an Electronic Questionnaire for Investigations Processing, executed by you under date June 23, 2009, in response to **"Section 13c. Employment Record:** Has any of the following happened to you in the last 7 years: 1. Fired from a job 2. Quit a job after being told you would be fired 3. Left a job by mutual agreement following charges or allegations of misconduct 4. Left a job by mutual

[1] Department Counsel changed the wording from that shown in HE I, to conform to the evidence presented at the hearing. The adjusted wording is shown at paragraph 1.d, above. (Tr. 213-214**)**

agreement following notice of unsatisfactory performance 5. Left a job for other reasons under unfavorable circumstances 6. Laid off from job by employer?" You answered "No" and deliberately failed to disclose that you left employment with [company name] in 2003 under unfavorable circumstances.

The parties agreed to a stipulation of fact, forwarded to me by email from Applicant's counsel, dated October 25, 2011. They agreed that Applicant's job duties, while he was employed at company B and working on an AGA contract, included downloading software without performing virus checks (SOR subparagraph 1.c (i)) specifically to study malicious code. The stipulation also included a statement by counsel for the AGA, that he "could not confirm Applicant's claims that each time he downloaded software without running a virus scan was specifically authorized." The stipulation is marked Hearing Exhibit II.

I granted Applicant's request that I take administrative notice of a federal statute, Title 18 U.S.C. § 2256, defining child pornography.

## Findings of Fact

Applicant's admissions to the SOR allegations are incorporated herein as findings of fact. After a thorough review of the pleadings and the evidence, I make the following additional findings of fact**.**

Applicant is 31 years old. As of the date of his 2009 security clearance application, he had never been married and had no children. He earned a bachelor's degree in computer science in 2005. From 2001 to 2003, when Applicant was 21 to 23 years of age, he worked for a defense contractor (company A). Initially, he was a help desk coordinator, and later a field representative. He started working for his current employer, a defense contractor (company B), in 2005. He is a reverse engineer. He was granted a top secret security clearance with sensitive compartmented information access (TS/SCI) in approximately 2006. Applicant's access to classified information was revoked in March 2009 following a security interview by another government agency (AGA). In December 2009, his personnel security clearance was suspended based on the AGA revocation. (GE 1-3; AE A; Tr. 117, 130)

### Guideline M, Use of Information Technology Systems

In 2001, Applicant's first job at company A was help desk representative. His computer was provided by company A, but he was not aware at the time if it was government-furnished equipment (GFE). He and other workers spent time browsing the Internet on their work computers, which were not classified systems. (Tr. 31) At some point, two supervisors told the workers that they were to stop using the Internet during work hours, because it interfered with productivity. In his 2008 security interview, Applicant explained that he circumvented this restriction by channeling his web access

through his home computer so that it did not appear as Internet activity on his work computer. He testified, “So, I took steps to use this VPN [virtual private network] access, to hide my traffic, so it did not look like I was browsing the Internet…” His supervisor discovered his violations several times but did not report him. Applicant's witness (W1), who worked with him at the company A help desk and later as a field representative, testified that the company had a policy against accessing the Internet during duty hours, but everyone used it, including the supervisor. (Tr. 27-30, 51) Applicant spent about 25 percent of his work day browsing the Internet. Applicant admitted during his AGA interview that he also attempted to access his office computer from his home computer, but was unable to access it. Applicant's witness (W1) testified that accessing a work computer from home was not authorized. (Tr. 54) (GE 3; Tr. 27-31, 51, 54; 128-131)

While working at company A, Applicant had access to a list of more than 200 Internet protocol (IP) addresses of DoD computers. He sent the list to his home computer and then used the list to try to access the DoD computers from his home computer. He successfully gained entry to approximately 10 to 15 computers. He did not attempt any further intrusion, because he only did it to be able to say he could. W1 testified that sending these addresses to a home computer was unauthorized. He also stated that using the addresses to access DoD computers was unauthorized. (GE 3; Tr. 55-56)

In about 2002, when Applicant worked for company A as a field representative, he trained soldiers to operate computer systems, use Common Access Cards (CAC) cards, and troubleshoot. Applicant assisted soldiers both by traveling to their DoD locations, and also by using VPN access to assist the soldier remotely, while he was physically located at his office. During his AGA interview, Applicant stated he used soldiers’ accounts for personal Internet browsing to check his home email, look at the news, and visit websites. This method prevented company A from detecting that he was violating company rules against Internet browsing during duty hours. The soldiers were unaware that he was browsing using their accounts. Applicant testified that he did not knowingly violate the policies of any DoD installations where he worked in person. W1 testified that the policies at some bases allowed them to use the Internet, and others did not, and that when the base authorized access, there would be no reason to use a soldier’s account to access it. (GE 2, 3; Tr. 32-38, 53, 121, 124, 138-144, 147-151)

During his travels, Applicant was provided with a laptop computer, software, and five CACs to use during training, if needed. W1 testified that the CACs contained unique serial numbers, and were treated as controlled items. However, company A did not control them well, and the serial number of each distributed card was not recorded. The security surrounding CACs is now much stricter than it was in the 2001-2003 timeframe. W1 was not asked to return any material when he left, other than his laptop. When Applicant left company A, he returned the laptop, but not the five CAC cards. In about 2004 or 2005, six months to one year after he left company A, he realized he had the CACs. In approximately 2007, he disabled the chips in the cards, cut the cards with scissors, and disposed of them in the trash. Company A never asked him to return

them. He did not call the company once he discovered them because he was embarrassed that he still had them. (GE 3; Tr. 32-36, 121, 124, 147-151)

Applicant left company A in 2003, returned to college, and completed his degree in 2005. He then began a full-time position with the defense contractor (company B), where he currently works. In March 2008, AGA administered a polygraph to Applicant. It also conducted an interview, during which Applicant provided details about his work for the agency. During this interview, Applicant stated he did not have an account that allowed him to use the Internet at company B, but his supervisor allowed him to use the supervisor's password and user ID to perform work functions. While using his supervisor's account, he also used the Internet to access technology blogs, news sites, and video game sites. During the interview, he estimated he spent ten percent of his day using the Internet, although at the hearing, he testified that this was an overestimate. Applicant's direct supervisor at company B from 2007 to 2009 submitted a letter stating it was standard practice within their work group to share credentials on the unclassified network. Applicant was given his supervisor's unclassified login information so that he could perform work functions, and "personal activities as outlined in agency policy." He noted, however, that in 2008, an internal investigation determined that the practice was found to be in violation of policy and it was discontinued. (GE 2, 3; AE C; Tr. 161-164)

Applicant's second witness (W2) worked for company B from 2005 to the present. He has held a TS/SCI for more than ten years. He has known Applicant at company B since 2007 and was his first- and second-level supervisor. Applicant was in the top five to ten percent of employees in their shop. He testified that Applicant's job included uploading software that contained viruses, without scanning it, because his job was to analyze malware and viruses. This action was within his job responsibilities, authorized by AGA, "and probably in the statement of work." (Tr. 57-68)

Applicant's direct supervisor at company B from 2007 to 2009 provided a letter stating that Applicant's official duties included analyzing malicious computer code, which required placing the code on computer systems that are designed for such analysis. "These systems are not connected to any United States Government agency networks…and have anti-virus software installed…" He also noted that company B allowed Applicant to use his supervisor's login information to perform technology research, check emails, and meet timesheet regulations. This was standard operating procedure at the time, and the government's contracting officer technical representative (COTR) approved it. He confirmed W2's statement that this practice was found to violate policy, and was discontinued. Applicant's former supervisor recommends him, noting that his work has benefitted U.S. security. As noted in the parties' stipulation, the AGA counsel agreed that Applicant's job "included downloading software without performing virus checks, specifically for the purposes of malicious code software study," although he could not confirm that each download was specifically authorized. (GE 2; AE C; HE II; Tr. 151-152)

During his security interview with AGA, Applicant stated that he brought items to his job at company B, including password-cracking software, rainbow tables, source code, and key generators. Applicant testified that he was authorized to bring these items to work by his chain of command, and did not bring in such items without permission. (Tr. 94) At times, certain software such as password-cracking software, could not be purchased legally for security reasons. He stated in his 2008 interview that he brought to work approximately 20 DVDs containing illegally obtained software that was required for his tasks and supported operational needs. In his 2010 statement, he said he "obtained downloads of this nature approximately twelve times between 2006 and 2009 on various occasions with the knowledge and consent of my supervisors." When he advised his supervisor and agency personnel of the legal constraints on obtaining such software, he was sometimes told to continue, and other times, not. He complied with these instructions. (GE 2, 3; Tr. 153-157)

Between 1995 and 2007, when Applicant was in high school, college, and working, he was 15 to 27 years old. He admits that, during those years, he downloaded material from the Internet illegally, without paying for it. The items included software applications, games, music, and movies for his personal use. During a security interview with AGA in March 2008, he estimated the value of these items to be between $300,000 and $500,000. However, in his statement of 2010, he described the value as approximately $200,000. He estimated the value of two of the software applications alone was $10,000. In 2008, he had approximately $2,000 to $3,000 worth of software on his home computer that he had obtained illegally. He also stated that from 2005 to 2008 he illegally downloaded movies, but less frequently, and also downloaded software and games. (GE 2, 3; Tr. 173-178)

As of 2008, his most recent illegal downloads included music in 2006 and a movie in 2007. At the hearing, he stated he "probably" downloaded a few items in 2008, and his last illegal download was approximately 2009. He noted that he had "an edgy sense of accomplishment" from illegal downloading in his "early years." However, he now has the funds to buy the items. "I realized I had a large collection of crap that I had acquired illegally, and it didn't -- I mean, most of it just sat and had no purpose, no intent, it was just get it (*sic*), to have it, and that was pointless." His feeling of guilt about his illegal activities after his AGA interviews also influenced him to stop illegally downloading. Currently, Applicant hosts "LAN parties" with friends, where each person needs a copy of the same video game, and Applicant pays for the copies he provides to his friends. (GE 2, 3; Tr. 173-178)

Applicant informed the AGA interviewer in 2008 that about three to four times per week, he viewed 40 to 50 pornographic images online. He did not purposefully use his work computer to view pornographic images. If his friends sent emails to his work computer that contained pornographic images, they used a code in the subject line to indicate he should only open it on his home computer. He stated he might have accessed links sent by friends that led to pornographic images on his work computer. If he did, he would close them and forward to his home computer to view at home.

Applicant believed that some of the images he viewed were of girls less than 18 years old.[2] He guessed that the youngest girl he had viewed online was approximately 13 years old. He estimated during his interview that about 10 percent of his viewing is of girls about 15 years of age. At the hearing, he clarified that this was an overstatement, and that he meant ten percent of the sites he accessed had "objectionable" images. (GE 3; Tr. 207-208)

At the hearing, Applicant testified that he surfs free pornography sites, primarily using pornography aggregators. He has not knowingly sought sites that include underage females. If he came across images he thought were inappropriate because the girls were underage, he would "move on." In the past, he has purchased pornography, but not child pornography. He also stated that he used the term "babysitters" as a search term on pornography aggregator sites. He knew that the "babysitters" term carried the greatest risk for returning images of minors, and it occurred to him to stop using it. However, he continued to use it. (AE G, H I, J; Tr. 178-187, 205-208)

**Guideline E, Personal Conduct**

The record of Applicant's 2008 AGA security interview states, **"**SUBJ was given a bag with a laptop, software and CAC cards when he traveled. Subject stated that he left under unfavorable circumstances and only returned the laptop." The SOR alleges Applicant falsified his 2009 security clearance application because he failed to disclose that he left his job with company A under unfavorable circumstances. Applicant testified that he did not leave under unfavorable circumstances, and never received unfavorable comments based on his work at company A. He informed his supervisor about one month before his departure that he planned to leave to return to school full time. He testified that he had performed well, and provided a letter showing that before he left he was offered a prospective bonus. However, he admitted to the AGA investigator that he had a contentious relationship with his immediate supervisor. In addition, on his last day, he wrote a letter to management:

> I had seen – observed some bad behavior of our – our supervisors lying to our customers, deceiving them, and doing things improperly, lying to us, and so, I spelled this out in a scathing letter to those people, you know, to all of them in my management chain, who had contacts to this, and wrote them a letter on my last day. (Tr. 125)

Applicant believes when he informed the interviewer of his negative relationship with his supervisor, she interpreted it as Applicant leaving under unfavorable circumstances. The record contains no other information indicating that Applicant left the job under unfavorable circumstances. (GE 3; AE B; Tr. 120-128, 135)

[2] Title 18 USCS § 2256 generally defines child pornography as a visual depiction of minors (under 18) engaged in sexually explicit conduct.

## Character Evidence

The division head for Applicant's current employer provided a character reference. He has been Applicant's second-level supervisor for two years. He believes some of Applicant's past conduct, such as illegally downloading software, games, and music, resulted from immaturity. It also stemmed, in his opinion, from an "environment where 'administrative obstacles' prevent/delay critical mission execution/support and, finally, due to a pervasive culture that preached the wrong message." He believes Applicant has made mistakes, but has matured, and recommends him for a security clearance. (AE D)

A friend of Applicant, who has been his coworker since 2007, submitted a character reference. He ascribes Applicant's "history of pirated software" to "moral immaturity." Applicant now acquires software licenses legitimately and tries to reform his friends of their pirating habits. He has personal experience with Applicant's same supervisor, who described that "operational necessities," such as using a supervisor's account, were "verbally condoned by the government supervisors who felt overburdened with bureaucratic hardships in the face of a rapidly evolving operational environment." (AE E)

On his performance evaluations from 2006 to 2008, Applicant generally received 4 or 5 in his tasks, and overall was awarded a 5 (Exceptional Performance). He was described as a valuable team member who did an outstanding job. His 2009 evaluation for security states that he "protects proprietary info by adhering to internal security policies (protects passwords, secures & destroys proprietary docs, locks workstation)." In 2010, his overall rating was "4" and he was described as an outstanding team member. Company A recognized him for outstanding performance in 2001 and 2003, He also received letters of recognition from company B in 2007 and 2008. In 2008, he and other team members were recognized by the government agency his company supported. (AE B, F; Tr. 118-120)

## Policies

Each security clearance decision must be a fair, impartial, and commonsense determination based on examination of all available relevant and material information, and consideration of the pertinent criteria and adjudication policy in the revised AG.[3] Decisions must reflect consideration of the "whole-person" factors listed in ¶ 2(a) of the Guidelines.

The presence or absence of disqualifying or mitigating conditions does not determine a conclusion for or against an applicant. However, specific applicable guidelines are followed when a case can be so measured, as they represent policy

[3] Directive 6.3.

guidance governing the grant or denial of access to classified information. 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 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. Additionally, the Government must be able to prove controverted facts alleged in the SOR. If the Government meets its burden, it falls to applicants to refute, extenuate or mitigate the Government's case. Because no one has a "right" to a security clearance, applicants bear a heavy burden of persuasion.[5] A person who has access to classified information enters a fiduciary relationship based on trust and confidence. The Government has a compelling interest in ensuring that applicants possess the requisite judgment, reliability, and trustworthiness to protect the national interest as his or her own. The "clearly consistent with the national interest" standard compels resolution of any reasonable doubt about an applicant's suitability for access to classified information in favor of the Government.[6]

## Analysis

### Guideline M, Use of Information Technology Systems

AG ¶ 39 expresses the security concern about use of information technology 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, or protection of information.

AG ¶ 40 describes disqualifying conditions that could raise a security concern, including the following relevant conditions:

---

[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;* Revised Adjudicative Guidelines, ¶ 2(b).

(a) Illegal or unauthorized entry into any information technology system or component thereof;

(c) use of any information technology system to gain unauthorized access to another system or to a compartmented area within the same system;

(e) unauthorized use of a government or other information technology system; and

(f) introduction, removal, or duplication of hardware, firmware, software, or media to or from any information technology system without authorization, when prohibited by rules, procedures, guidelines or regulations.

From 2001 to 2003, while an employee of a federal contractor (company A), Applicant worked in a help-desk capacity and as a field representative. Despite having been told not to use the Internet by his supervisor, he used VPN to hide the fact that he was browsing the Internet on his work computer. He spent 25 percent of his day using the Internet. He attempted to access his work computer from his home computer, which was not authorized. He sent approximately 200 DoD IP addresses from his work computer to his home computer, which was not authorized. He used the addresses to see if he could access the DoD computers from his home computer, which was not authorized. He did not return controlled government CAC cards when he left his employment at company A. He used soldiers' computer accounts at DoD installations to browse the Internet, without their knowledge, at times when the installation did not authorize such use. He used their accounts to prevent his employer from becoming aware that he was accessing the Internet during duty hours. Applicant admits he received emails from friends on his work computer that contained pornographic images and/or links to such images, and he may have accessed such links on his work computer. Disqualifying conditions AG ¶ 40(a), (c), (e) and (f) apply.

Starting in 2005, Applicant worked for another federal contractor (company B). His job involved, among other tasks, working with malicious code and detecting viruses. He engaged in activities that, under other circumstances, would be unauthorized, including *inter alia*: failing to perform virus checks before loading software onto a government network or computer; using password-cracking software; using his supervisor's account or password; and illegally obtaining certain software. However, as stated by his supervisors, these tasks were integral to his job, were authorized, and even required by the government sponsor. Applicant's actions, alleged at subparagraphs 1.c (i) to 1.c (iv), are not disqualifying.

AG ¶ 41 provides the following relevant mitigating conditions:

(a) so much time has elapsed since the behavior happened, or it happened under such unusual circumstances, that it is unlikely to recur

and does not cast doubt on the individual's reliability, trustworthiness, or good judgment;

(b) the misuse was minor and done only in the interest of organizational efficiency and effectiveness, such as letting another person use one's password or computer when no other timely alternative was readily available; and

(c) the conduct was unintentional or inadvertent and was followed by a prompt, good-faith effort to correct the situation and by notification of a supervisor.

Applicant engaged in conduct that was unauthorized, and violated his supervisor's instructions, at company A, from 2001 to 2003. This behavior is not recent; however, the varied type of infractions, their frequency, and the deliberate nature of Applicant's violations outweigh their distance in time. His conduct did not occur under unusual circumstances, but in the course of his routine duties, and in the same field in which he currently works. Moreover, he deliberately used techniques that would hide his actions from his supervisors. Unlike his position at company B, many of Applicant's infractions at company A were not done in response to organizational needs or contract requirements. They were not inadvertent, but deliberately done for his purposes, often simply to see if he could outwit the system. Such conduct raises questions about Applicant's trustworthiness and judgment. AG ¶ 41 (a), (b) and (c) do not 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. 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.

AG ¶ 16 describes conditions that could raise a security concern and may be disqualifying. The following conditions are relevant:

(a) deliberate omission, concealment, or falsification of relevant facts from any personnel security questionnaire, personal history statement, or similar form used to conduct investigations, determine employment qualifications, award benefits or status, determine security clearance eligibility or trustworthiness, or award fiduciary responsibilities;

(d) credible adverse information that is not explicitly covered under any other guideline and may not be sufficient by itself for an adverse determination, but which, when combined with all available information 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. This includes but is not limited to consideration of…

(3) a pattern of dishonesty or rule violations; and,

(4) evidence of significant misuse of Government or other employer's time or resources.

The AGA interview report states that Applicant left his job with company A under unfavorable circumstances, but it provides no further explanation. Applicant's "scathing letter" and his contentious relationship with his supervisor indicate that he may have had interpersonal problems at company A. On the other hand, Applicant was commended for his work there, and his employer offered him a bonus in the month before he left the company. The record is not sufficient to find that unfavorable circumstances surrounded Applicant's departure from company A. I conclude that the allegation of deliberate falsification is not supported by substantial evidence. AG ¶16 (a) does not apply.

Applicant's conduct, alleged under Guideline M, is also cross-alleged under Guideline E. Several of Applicant's activities are disqualifying under Guideline E. At company A, he accessed the Internet on his work computer. Initially, company A allowed this activity; however, his supervisor later prohibited Internet use. Although he was not authorized to Internet-browse during the work day on company computers, Applicant continued to do so, violating the supervisor's prohibition. He compounded his violation by deliberately using techniques to hide his prohibited activities from his employer. He wasted significant government time and resources by spending approximately 25 percent of his day on personal Internet activities. Applicant disregarded rules regarding Internet use, misused company time, and hid his infractions. AG ¶ 16(d) (3) and (4) apply.

From 1995 to 2009, Applicant illegally downloaded movies, games, music, and software applications from the Internet without paying for them. He gradually curbed his illegal activity, and testified he has not engaged in this activity since 2009. The value of the material he downloaded from 1995 to 2007 was at least $200,000. Applicant's viewing of child pornographic is also disqualifying under Guideline E. Whether child pornography constituted more than ten percent, or less than ten percent of his total pornography viewing does not mitigate the fact that he illegally view images of females who he believed to be less than 18 years of age. His conduct is recent, because he continues to use the search term that he characterizes as most likely to

result in images of minor females. His actions show a willingness to violate the law. AG ¶ 16(d) (3) applies.

AG ¶ 17 provides conditions that could mitigate security concerns under the Personal Conduct guideline. The following condition is 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.

At company A, Applicant knowingly engaged in prohibited conduct, as discussed under Guideline M. His offenses are not minor, because he used company resources in a prohibited manner for a substantial amount of his workday, and deliberately sought to hide his behavior from his employer. His violations were not infrequent, but occurred over a period of years. He continues to work in the same field in which he engaged in these activities, so such behavior could recur. The fact that some of his conduct is not recent, is outweighed by his troubling willingness to break rules simply to see if he could, to put his own desires ahead of the Government's, and ahead of the law. His actions indicate poor judgment and untrustworthiness. AG ¶ 17(c) does not apply.

**Whole-Person Analysis**

Under the whole-person concept, an administrative judge must evaluate the Applicant's security eligibility by considering the totality of the Applicant's conduct and all the relevant 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 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.

Some of Applicant's unauthorized activity occurred when he was in high school, college, and working at company A, and can be ascribed to his immaturity. Moreover,

his actions at company B are not at issue because the nature of his job required him to engage in computer activity that would ordinarily be prohibited, such as loading malicious code without virus scans, in order to detect vulnerabilities. However, at company A, Applicant abused his position of trust when he used others' accounts for his own purposes, violated his supervisor's prohibitions, sent DoD information to his home computer, and engaged in other unauthorized activities. The frequency and variety of ways in which Applicant engaged in unauthorized activities is troubling. Each time he knowingly engaged in prohibited conduct, he placed his own desires above the Government's need for reliable and trustworthy conduct.

Applicant's illegal downloading of software, music, and movies extended over a period of 14 years, until 2009, when he was 29 years of age. Finally, he continues to use a search term that he knows often brings up images he believes to be of underage females. This conduct raises doubts as to his trustworthiness and good judgment.

Overall, the record evidence fails to satisfy the doubts raised about Applicant's suitability for a security clearance. For all these reasons, I conclude Applicant has not mitigated the security concerns arising from the cited adjudicative guidelines.

## Formal Findings

| | |
|---|---|
| Paragraph 1, Guideline M | AGAINST APPLICANT |
| Subparagraphs 1.a – 1.b | Against Applicant |
| Subparagraphs 1.c (i) - (iv) | For Applicant |
| Subparagraphs 1.d – 1.h | Against Applicant |
| Paragraph 2, Guideline E | AGAINST APPLICANT |
| Subparagraph 2.a | Against Applicant |
| Subparagraph 2.b | For Applicant |

## Conclusion

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

RITA C. O'BRIEN
Administrative Judge