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

| | | |
|---|---|---|
| In the matter of: | ) | |
| | ) | |
| | ) | ISCR Case No. 08-08260 |
| SSN: | ) | |
| | ) | |
| Applicant for Security Clearance | ) | |

## Appearances

For Government: D. Michael Lyles, Esquire, Department Counsel
For Applicant: *Pro se*

October 15, 2009

## Decision

HOGAN, Erin C., Administrative Judge:

Applicant submitted his Electronic Questionnaire for Investigations Processing (e-QIP) on February 27, 2008. On or before April 27, 2009, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) detailing the security concerns under Guideline E, Personal Conduct; Guideline M, Use of Information Technology Systems; and Guideline D, Sexual Behavior. (The SOR was undated. The memorandum forwarding the SOR to Applicant is dated April 27, 2009, and is used to estimate the date when the SOR was issued.) The action was taken under Executive Order 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 revised adjudicative guidelines (AG) promulgated by the President on December 29, 2005, and effective within the Department of Defense for SORs issued after September 1, 2006.

On May 26, 2009, Applicant answered the SOR and requested a hearing before an administrative judge. Department Counsel was ready to proceed on July 15, 2009. The case was assigned to me on July 24, 2009. On August 3, 2009, a Notice of Hearing was issued, scheduling the hearing for August 26, 2009. The case was heard on that date. The government offered four exhibits which were admitted as Government

Exhibits (Gov) 1 – 4. Applicant testified and submitted no documents. The transcript was received on September 10, 2009. Based upon a review of the case file, pleadings, exhibits, and testimony, eligibility for access to classified information is granted.

## Findings of Fact

In his Answer to the SOR, Applicant admits the allegations in SOR ¶¶ 1.a and 2.a. He denies the remaining SOR allegations.

Applicant is a 39-year-old software engineer for a Department of Defense contractor who seeks to maintain his security clearance. He has been employed in his current position since November 2007. He has held a security clearance since March 2003. He is a high school graduate and has taken some college courses. He is single and has two daughters, ages 17 and 10. (Tr at 5-6; Gov 1)

From August 2005 to March 2007, Applicant worked as a network technician for another defense contractor located in another state. He applied for and was granted a security clearance for the first time in this job. When he first started working for the defense contractor, Applicant occasionally accessed the internet to use his personal e-mail accounts during work hours. He admits that he responded to e-mails from dating and adult sites that he had joined. He insists the adult sites did not contain pornography. He also received SPAM e-mails that contained pornographic sites. A work computer scan revealed that Applicant had been accessing the internet for personal reasons. On September 29, 2005, Applicant's supervisor verbally counseled him for unacceptable internet use. The usage logs indicated Applicant used the internet for unacceptable reasons on September 18, 2005, September 28, 2005, and September 29, 2005. The specific unacceptable reasons were not described. (Tr at 17-18, 33-41; Gov 4 at 2; Response to SOR, dated May 26, 2009)

On June 20, 2006, Applicant received a warning letter for inappropriate internet use. The letter does not provide the specific details of the unacceptable internet use other than Applicant was using customer-provided resources to access the internet for personal use. The customer complained about Applicant's excessive and unacceptable internet usage on February 15, 2006, May 1, 2006, and June 14, 2006. The warning letter stated that Applicant violated the company's Network Systems Policies: PS-ISS-150 Acceptable Use Policy, Business Practice Council Guideline Use of Electronic Communications, and Section 406 Performance Improvement Policy – Section 2, specifically:

> 2.21 Violating customer/contract compliance and business ethics policies.
>
> 2.23 Engaging in conduct which causes embarrassment to the company or potentially disparages its image.

Applicant was warned that the excessive amount of time spent on the internet was not warranted, and reflected negatively on his overall performance and the

company. He was warned that future occurrences would result in further disciplinary action up to and including termination of employment. The warning letter was placed in Applicant's file for one year. During that time, he was not eligible to receive a merit increase or to participate in recognition programs. (Gov 4)

Applicant admits that he received this warning letter but denies the inappropriate internet usage at work included accessing sites related to dating and pornography as alleged in SOR ¶ 2.a. He admits to accessing the internet while at work to check basketball scores. Nothing in the record evidence indicates the basis for the warning letter was Applicant accessing web-sites for dating or pornography while at work. (Tr at 18 – 20, 41; Response to SOR, dated May 26, 2009)

On March 21, 2007, Applicant was contacted by an investigator with the local police department and asked to come in for questioning. He was questioned about solicitation of a minor over his home computer in February 2007. Applicant denies any knowledge of soliciting a minor over the internet. During the time period in question, he allowed an acquaintance in his apartment complex to use his computer on occasion. The computer was his personal lap top and was not a government computer. On the day he was called in for questioning, the local police department obtained a search warrant and seized Applicant's personal lap top, equipment, and several disks. After he was questioned, Applicant was free to leave. He was not arrested or charged with any offense. (Tr at 21-23, 43-47; Gov 2; Gov 1, section 22; Gov 3; Response to SOR)

On March 23, 2007, Applicant's manager called him on his day off. His manager told him that someone from the local police department contacted the office and told them that Applicant was arrested on March 21, 2007, for soliciting a minor over the internet. Applicant said he was willing to come in to work to discuss the matter. He told his manager that he was called in for questioning by police but not arrested. He denied soliciting a minor over the internet. Applicant was placed on administrative leave because the customer did not want publicity. On March 27, 2007, Applicant was asked to resign. He resigned because he believed that he had no choice but to resign or be fired. In April, the police department returned his computer and equipment to him. He was never charged with an offense and never provided any documentation about the incident. (Tr at 24 – 26, 47; Gov 2; Gov 3; Response to SOR)

From March 2007 to November 2007, Applicant was unemployed. He lost his apartment and everything in it. He moved back to his home state and was hired by his current employer in November 2007. On February 27, 2008, he completed his e-QIP application. In response to section 22: Your Employment Record, Applicant indicated that he left a job by mutual agreement following allegations of misconduct with regards to his previous employer. He provided a detailed explanation of the circumstances that led to his resignation. (Gov 1, Sec 22)

Applicant has worked for his current employer without incident. Aside from when he was called in for questioning in March 2007, he has had no other involvement with law enforcement. (Tr at 51)

## Policies

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

These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, these guidelines are applied in conjunction with the factors listed in the adjudicative process. The administrative judge's overarching adjudicative goal is a fair, impartial, and commonsense decision. According to AG ¶ 2(c), the entire process is a conscientious scrutiny of a number of variables known as the "whole person concept." The administrative judge must consider all available, reliable information about the person, past and present, favorable and unfavorable, in making a decision.

The protection of the national security is the paramount consideration. AG ¶ 2(b) requires that "[a]ny doubt concerning personnel being considered for access to classified information will be resolved in favor of national security." In reaching this decision, I have drawn only those conclusions that are reasonable, logical, and based on the evidence contained in the record.

Under Directive ¶ E3.1.14, the government must present evidence to establish controverted facts alleged in the SOR. Under Directive ¶ E3.1.15, the applicant is responsible for presenting "witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by applicant or proven by Department Counsel. . . ." The applicant has the ultimate burden of persuasion as to obtaining a favorable security decision.

A person who seeks access to classified information enters into a fiduciary relationship with the government predicated upon trust and confidence. This relationship transcends normal duty hours and endures throughout off-duty hours. The government reposes a high degree of trust and confidence in individuals to whom it grants access to classified information. Decisions include, by necessity, consideration of the possible risk the applicant may deliberately or inadvertently fail to protect or 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.

Section 7 of Executive Order 10865 provides that decisions shall be "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." *See also* EO 12968, Section 3.1(b) (listing multiple prerequisites for access to classified or sensitive information).

## Analysis

### Guideline E, Personal Conduct

The security concern relating to the guideline 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 following Personal Conduct Disqualifying Conditions (PC DC) potentially apply to the facts of this case:

PC DC ¶ 16(c) (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)

PC DC ¶ 16(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: (1) untrustworthy or unreliable behavior to include breach of client confidentiality, release of proprietary information, unauthorized release of sensitive corporate or other government protected information; (2) disruptive, violent, or other inappropriate behavior in the workplace; (3) a pattern of dishonesty or rule violations); (4) evidence of significant misuse of Government or other employer's time or resources)

PC DC ¶ 16(c ) and ¶ 16(d) apply with respect to SOR ¶¶ 1.a and 1.b. Applicant was verbally counseled in September 2005 for unacceptable internet use by his employer. He admits that he used his work computer for personal use and accessed dating and adult web-sites during duty hours. He denies accessing pornographic web-sites but claims pornographic web-sites were sent as SPAM e-mail. Although he was warned to restrict his internet use at work for business purposes only, he received a written warning for inappropriate use of a business computer between February 2006 to June 2006. The specifics describing the inappropriate use were not provided in the record evidence. Applicant admits to checking basketball scores while at work. He feels

that he was singled out because other co-workers were doing the same thing. There is no record evidence to support the premise that he accessed dating and pornographic web-sites on these occasions.

SOR ¶1.c is found for Applicant. There is no evidence Applicant used a government computer while at the customer work site to solicit a minor over the internet as the allegation alleges. Applicant admits he was questioned by police about the use of his home computer to solicit a minor over the internet while at home. He denies the allegation. He cooperated with law enforcement when called in for questioning. His computer, computer equipment, and computer disks were seized pursuant to a search warrant. Nothing illicit was found on his computer or computer disks. He was not arrested. Applicant claims he let an acquaintance in his apartment complex use his computer during the same timeframe that the alleged solicitation occurred. (Note: The file contains no evidence pertaining to the alleged solicitation which was the basis for calling in Applicant for questioning.) The record evidence contains no information from independent sources or law enforcement that contradict Applicant's testimony. No witnesses were called to establish the alleged offense. Applicant fully disclosed the incident when he completed his e-QIP application in February 2008. In fact, he is the only source in the record evidence describing this incident. Being called in for questioning does not mean an individual committed the offense. There is insufficient evidence to establish that Applicant solicited a minor over the internet on his home computer.

A *prima facie* case is found with respect to SOR ¶¶ 1.d and 1.e. Applicant was questioned by the local police department in March 2007 regarding accessing the internet from his personal computer for the purposes of soliciting a minor. He was subsequently placed on administrative leave and eventually asked to resign. However, the record evidence does not establish Applicant committed the offense that the police questioned him about.

The security concerns raised under personal conduct are mitigated. I find the following Personal Conduct Mitigating Conditions (PC MC) apply to Applicant's case:

PC MC ¶ 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)

PC MC ¶ 17 (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 factors that caused untrustworthy, unreliable, or other inappropriate behavior, and such behavior is unlikely to recur)

While Applicant was counseled on two occasions for misuse of his work computer in 2005 and 2006, he has not repeated the conduct since that time. He has been employed since November 2007 with his current employer and has no issues

regarding inappropriate use of his work computer. While Applicant was called in for questioning about soliciting a minor on his personal computer, he was never arrested or charged with a crime. He denies the allegation and there is no record evidence that contradicts his testimony. In fact, all of the government's evidence consists of testimony provided by Applicant. The allegations caused Applicant to lose his job. He resigned but felt he had no alternative. The circumstances are such that it does not cast doubt on Applicant's reliability and trustworthiness. Considering all that Applicant has been through, he is unlikely to repeat such conduct.

**Guideline M, Use of Information Technology Systems**

The trustworthiness concern relating to the guideline for Use of Information Technology Systems is set out in AG ¶ 39 which states,

> 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 following disqualifying conditions apply under Guideline M (M DC) in Applicant's case with respect to SOR ¶¶1.a, and 1.b:

M DC ¶ 40(e) (unauthorized use of a government or other information technology system)

While Applicant believes he was singled out for punishment for his second offense when he received the written warning letter, he admits that he violated company policies pertaining to internet use while at work. The warning letter Applicant received stated the specific company policies Applicant violated pertaining to computer use.

The issues pertaining to Use of Information Technology Systems can be mitigated (M MC). M MC ¶ 41(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) applies to Applicant's case. More than three years have passed since this incident. Since that time, Applicant has not been involved in any similar incidents. Applicant mitigated the Guideline M concern.

The allegations in SOR ¶¶ 1.c, 1.d, and 1.e are not relevant to the Guideline M allegation because they ultimately did not involve the use of a work computer and did not occur in the work place.

**Guideline D, Sexual Behavior**

The security concern raised under the Sexual Behavior guideline is set forth in ¶12 of the Revised Adjudicative Guidelines:

> 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 government did not establish its case with respect to SOR ¶ 1.c for the reasons discussed above under personal conduct. The government did not establish its case with respect to SOR ¶ 1.b because there is no evidence that Applicant's inappropriate internet usage at work between February 2006 to June 2006 included accessing web-sites related to dating and pornography. Applicant admits to accessing adult and dating web-sites on his work computer when he was verbally counseled in September 2005 which is the basis of SOR ¶ 1.a.

With respect to SOR ¶ 1.a, the following disqualifying condition is relevant to Applicant's case:

Sexual Behavior Disqualifying Condition ¶ 13(d) (sexual behavior of a public nature and/or that reflects lack of discretion or judgment). Accessing adult sites at the workplace indicates a lack of judgment on Applicant's part.

Concerns raised under Sexual Behavior can be mitigated. The following mitigating conditions potentially apply to Applicant's case. Sexual Behavior Mitigating Condition ¶ 14(b) (the sexual behavior happened so long ago, so infrequently, or under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or good judgment) applies. More than four years have passed since Applicant was warned about the inappropriate use of his work computer. There is no evidence that he used his work computer to access adult web-sites and pornography on the internet since September 2005. The conduct was not recent and does not cast doubt on Applicant's current reliability, trustworthiness, and judgment.

Applicant mitigated the concerns raised under sexual behavior.

**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.

I considered the potentially disqualifying and mitigating conditions in light of all the facts and circumstances surrounding this case. While Applicant was counseled by his previous employer on two occasions for inappropriate use of company computers, specifically for accessing the internet for personal reasons, he has not repeated such conduct in over three years. While he was questioned by police about soliciting a minor on his personal computer, he denies the allegation. The government did not prove this controverted allegation by substantial evidence. Applicant was never arrested or charged with any offense. Nothing illicit was found on his computer after it was seized pursuant to a search warrant. While Applicant resigned when asked to do so after his company learned that he was questioned by police, he felt he had no alternative but to resign. He has successfully worked in his current position since November 2007. Applicant mitigated the security concerns raised under Personal Conduct, Use of Information Technology Systems, and Sexual Behavior.

## 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 E: | FOR APPLICANT |
| Subparagraph 1.a: | For Applicant |
| Subparagraph 1.b: | For Applicant |
| Subparagraph 1.c: | For Applicant |
| Subparagraph 1.d: | For Applicant |
| Subparagraph 1.e: | For Applicant |
| Paragraph 2, Guideline M: | FOR APPLICANT |
| Subparagraph 2.a: | For Applicant |

| | |
|---|---|
| Paragraph 3, Guideline D: | FOR APPLICANT |
| Subparagraph 3.a: | 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.

ERIN C. HOGAN
Administrative Judge