DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 11-09056
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Candace L. Garcia, Esq., Department Counsel
For Applicant: *Pro se*

08/16/2013

Decision

COACHER, Robert E., Administrative Judge:

Applicant failed to mitigate the security concerns under Guideline M, use of information technology systems, and Guideline E, personal conduct. The Government failed to establish a disqualifying condition under Guideline D, sexual behavior, by substantial evidence. Applicant's eligibility for a security clearance is denied.

Statement of the Case

On March 15, 2013, the Department of Defense Office (DOD) issued Applicant a Statement of Reasons (SOR) detailing security concerns under Guideline M, use of information technology systems; Guideline D, sexual behavior; and Guideline E, personal conduct. DOD acted 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 adjudicative guidelines (AG), effective within the Department of Defense on September 1, 2006.

Applicant answered the SOR on April 15, 2013. He requested a hearing before an administrative judge. The case was assigned to me on June 11, 2013. The Defense Office of Hearings and Appeals (DOHA) issued a notice of hearing on June 27, 2013, with a hearing date of July 9, 2013. The hearing was convened as scheduled. The Government offered exhibits (GE) 1 through 4, which were admitted into evidence without objection. The Government's exhibit list was marked and accepted as hearing exhibit (HE) I. Applicant testified, but offered no exhibits or witnesses. DOHA received the hearing transcript (Tr.) on July 16, 2013.

Findings of Fact

In Applicant's answer to the SOR, he essentially denied all the allegations listed in the SOR. After a thorough and careful review of the pleadings, testimony, and exhibits, I make the following findings of fact.

Applicant is 42 years old. He is single, never married, and has no children. He has a high school diploma and has taken some college courses. He currently works for a defense contractor as a systems administrator. He began working for his current employer in January 2011. He retired from the Marine Corps as a master sergeant (pay grade E-8) in May 2010. He currently holds a security clearance.[1]

Applicant's conduct alleged in the SOR includes: (1) accessing wireless networks, without authorization, from 2006 to 2009, and taking a hard drive from work, without authorization, for personal use (SOR ¶¶ 1.a-1.b, 3.a-3.b); (2) engaging in voyeurism (SOR ¶ 2.a); and, (3) providing false information on his February 2011 security clearance application by failing to list his unauthorized accessing of wireless networks in 2006 to 2009, and by providing false information when responding to Government interrogatories in November 2012 by failing to disclose his unauthorized accessing of wireless accounts and viewing of private accounts (SOR ¶¶ 3.c-3.d).

In 2008, while still on active duty in the Marine Corps, Applicant's duties included repairing laptop computers. When work requirements demanded it, he took some of the laptop computers to his home to work on them. He did this on three to four occasions. All the laptops were unclassified and none contained classified software or information. In attempting to repair the computers he would replace the hard drives with his own personal hard drives so that he could get the machines working as quickly as possible. His supervisors acquiesced to his actions by letting him know that they wanted the computers fixed quickly. He was never disciplined or counseled for his action in taking the computers home and replacing the hard drives. He denied the version of events concerning this incident listed in an investigative report prepared by another government agency (AGA).[2]

[1] Tr. at 6-8, 27; GE 1.

[2] Tr. at 29, 33-35, 45-46; GE 4.

Applicant admitted to watching adult pornography on occasion in the past. He also stated that during an interview with AGA, when asked about voyeurism, he was referring to watching adult pornography. There is no evidence to suggest he watched adult pornography using government resources. He has not participated in watching live sex acts.[3]

Between 2006 and 2009, Applicant accessed the wireless networks of others on several occasions. On some occasions he connected to these networks through no affirmative action on his part. By default his computer would pick up the network of others. He would use these wireless networks to check his email account and browse the internet. He did not access anyone's private accounts on these occasions. There were other occasions, during the same timeframe, when Applicant actively penetrated other people's wireless networks by using "tools" to discover the passwords for the network. Once penetrated, he would access the network and again check his email and browse the internet. He did not have permission to access these networks. He stated that his reason for accessing these networks was out of curiosity. He admitted that what he did could be considered "hacking." He wanted to see if he could do it. He also admitted that he had reservations about using "tools" to retrieve passwords without authorization, but he did it anyway.[4]

In February 2011, Applicant filled out his security clearance application and was asked whether he had ever "illegally or without proper authorization entered into any information technology system." He answered "no" to this question. When he was asked why he did not list this information on his application, he stated, "I did not recall the incidents when I was completing this." I find this response not credible considering this specific topic was thoroughly addressed by AGA in July 2010. In November 2012, Applicant answered interrogatories sent to him by the Government and specifically stated that he accessed other people's wireless accounts using "tools" to determine their passwords. He also stated that he did not access the people's computers or open any of their files to retrieve personal information. His hearing testimony was consistent with his interrogatory answers.[5]

Policies

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

[3] Tr. at 38; GE 4.

[4] Tr. at 39-43, 51-52, 55, 64-66; GE 3, 4.

[5] Tr. at 42-43, 58-60; GE 1.

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, an "applicant is responsible for presenting witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by applicant or proven by Department Counsel, and has the ultimate burden of persuasion to obtain 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 that an applicant may deliberately or inadvertently fail to safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation as to potential, rather than actual, risk of compromise of classified information.

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 M, Use of Information Technology Systems

AG ¶ 39 expresses the security concern pertaining to 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 reliably 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 conditions that could raise a security concern and may be disqualifying. I have considered the following as potentially relevant:

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

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

Applicant admitted to "hacking" into people's wireless networks on multiple occasions between 2006 and 2009. He was not authorized to do so. However, concerning the other allegation stated in SOR ¶ 1.a, I conclude that there is insufficient evidence to support that he viewed the private accounts of others. There is also insufficient evidence to establish that he did not have authorization to take the computer hard drive home as alleged in SOR ¶ 1.b. I find that AG ¶ 40(a) applies to SOR ¶ 1.a in part.

I also have considered all of the mitigating conditions under AG ¶ 41 and I considered the following relevant:

(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.

Although Applicant's actions in "hacking" into other people's wireless network occurred from 2006 to 2009, the reason he gave for doing so (i.e., he was curious to see if he could do it) shows a lack of good judgment and casts doubt on his reliability and good judgment. AG ¶ 41(a) does not apply.

Guideline D, Sexual Behavior

AG ¶ 12 expresses the sexual behavior security concern:

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.

I have considered all of the sexual behavior disqualifying conditions under AG ¶ 13 and the following are potentially applicable:

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

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

Applicant testified that he used the term voyeurism to describe his acts of viewing adult pornography. This action does not subject him to coercion, exploitation, or duress. There is no evidence to indicate that his actions were of a public nature or lacked discretion. Neither of the above listed disqualifying conditions applies.

Guideline E, Personal Conduct

AG ¶ 15 expresses the security concern for 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 in this case. The following disqualifying condition is potentially applicable:

(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;

(b) deliberately providing false or misleading information concerning relevant facts to an employer, investigator, security official, competent medical authority, or other official government representative; and

(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; and,

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

Applicant's "hacking" to gain password access into others wireless networks indicates untrustworthy behavior. AG ¶ 16(c) applies to SOR ¶ 3.a in part (see earlier discussion concerning SOR ¶ 1.a). For the reasons stated above under Guideline D, no disqualifying conditions apply to SOR ¶ 3.b. Applicant's reliance on forgetfulness as an excuse for not answering the question about unauthorized access to computer systems on his security clearance application is not credible. AG ¶ 16(a) applies to SOR ¶ 3.c. The evidence does not support the allegation that Applicant was not truthful when he answered the Government's interrogatories. His testimony was consistent with his earlier answers. AG ¶¶ 16(a) and 16(b) do not apply to SOR ¶ 3.d.

The guideline also includes conditions that could mitigate security concerns arising from personal conduct. I have considered all of the mitigating conditions under AG ¶ 17 and found the following 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.

Failing to provide truthful and complete information on a security clearance application is never a minor offense. His untruthful answer casts doubt on his reliability, trustworthiness, and good judgment. AG ¶ 17(c) does not apply.

Whole-Person Concept

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

> (1) the nature, extent, and seriousness of the conduct; (2) the circumstances surrounding the conduct, to include knowledgeable participation; (3) the frequency and recency of the conduct; (4) the individual's age and maturity at the time of the conduct; (5) the extent to which participation is voluntary; (6) the presence or absence of rehabilitation and other permanent behavioral changes; (7) the motivation for the conduct; (8) the potential for pressure, coercion, exploitation, or duress; and (9) the likelihood of continuation or recurrence.

Under AG ¶ 2(c), the ultimate determination of whether to grant eligibility for a security clearance must be an overall commonsense judgment based upon careful consideration of the guidelines and the whole-person concept.

I considered the potentially disqualifying and mitigating conditions in light of all the facts and circumstances surrounding this case. I considered Applicant's service to the Marine Corps. I also considered his intentional, purposeful acts of "hacking" into other person's wireless networks. I also considered his reason for doing so-–because he wanted to see if he could do it---as an indicator of bad judgment. Applicant failed to meet his burden to mitigate the security concerns.

Overall, the record evidence leaves me with questions and doubts about Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude Applicant failed to mitigate the security concerns arising under Guideline M, use of information technology systems, and Guideline E, personal conduct The Government failed to establish a prima facie case under Guideline D, 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 M:	AGAINST APPLICANT
Subparagraph 1.a:	Against Applicant
Subparagraph 1.b:	For Applicant
Paragraph 2, Guideline D:	FOR APPLICANT
Subparagraph 2.a:	For Applicant
Paragraph 3, Guideline E:	AGAINST APPLICANT
Subparagraph 3.a:	Against Applicant
Subparagraph 3.b:	For Applicant
Subparagraph 3.c:	Against Applicant
Subparagraph 3.d:	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 grant Applicant's eligibility for a security clearance. Eligibility for access to classified information is denied.

_____
Robert E. Coacher
Administrative Judge