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

In the matter of: )
)
) ISCR Case No. 09-03490
SSN: )
)
Applicant for Security Clearance )

## Appearances

For Government: Francisco J. Mendez, Jr., Esq., Department Counsel
For Applicant: Riley C. Porter, Personal Representative

September 30, 2010

## Decision

COACHER, Robert E., Administrative Judge:

Applicant failed to mitigate the Government's security concerns under Guideline E, Personal Conduct and Guideline M, Use of Information Technology Systems. Applicant's eligibility for a security clearance is denied.

## Statement of the Case

On December 3, 2009, the Defense Office of Hearings and Appeals (DOHA) issued to Applicant a Statement of Reasons (SOR) detailing security concerns under Guideline E, Personal Conduct and Guideline M, Use of Information Technology Systems. DOHA 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).

Applicant answered the SOR on January 6, 2010, and requested a hearing before an administrative judge. On April 1, 2010, Department Counsel issued an amended SOR and served it on the Applicant. The amended SOR withdrew, renumbered, and added allegations.[1] Applicant answered the amended SOR on April 19, 2010. The case was assigned to me on June 15, 2010. DOHA issued a notice of hearing on June 16, 2010, and the hearing was convened as scheduled on July 14, 2010. The Government offered Exhibits (GE) 1 through 4, which were admitted without objection. Department Counsel's exhibit index is marked as Hearing Exhibit (HE) I. Applicant testified and presented one witness, but did not offer any exhibits. DOHA received the hearing transcript (Tr.) on July 26, 2010.

## Findings of Fact

In Applicant's answer to the SOR, he admitted ¶ 1.b and denied ¶¶ 1.a, 1.c, and 2.a. After a thorough and careful review of the pleadings and exhibits submitted, I make the following findings of fact.

Applicant is 22 years old. He is single and has never been married. Since 2008, he has worked as an information systems security engineer for a defense contractor. He received a bachelor's degree in information assurance in December 2009. He also holds an associate's degree in network technology that he received in May 2007. He has no military experience. He sought a security clearance from another government agency in 2007, but was denied.[2]

Applicant's conduct raised in the SOR includes: (1) gaining access to another person's computer system (computer hacking) and manipulating information or software on that system on several occasions between 2005 and 2007 (Applicant admits one instance in 2005, but denies the rest); (2) gaining unauthorized access to a local traffic signal's computer controls and subsequently altering an electronic traffic warning signal on more than one occasion (admitted); and, (3) making false statements to investigators on July 25, 2007 by failing to disclose his computer hacking activities (denied). The conduct alleged in (1) and (2) above was cross alleged as security concerns under both Guideline E (personal conduct) and Guideline M (use of information technology systems).

Since December 2005, when Applicant was 17 years old, he has engaged in basic computer hacking attacks. Applicant understands hacking as gaining unauthorized access to computer systems/networks. Although he claims never to have hacked into any government systems or networks, he developed his skills by targeting his friends systems and engaging in denial of service attacks on their computers. These attacks are accomplished by flooding a victim's computer system or network with

[1] Original SOR ¶¶ 1.a – 1.h and 1.j – 1.o were withdrawn; a new SOR ¶¶ 1.a and 1.c were added; original SOR ¶ 1.i was renumbered as SOR ¶1.b; original SOR ¶ 2.a was changed.

[2] Tr. at 27-28; GE 1, 4.

electronic information to boot the system offline. Additionally, he used another type of attack to gain access to user names and passwords. Applicant believes his friends consented to these attacks so they all could develop their hacking skills. He also believes no laws were broken, but he may have violated the terms of use established by the affected internet service provider.[3]

During 2005, Applicant also engaged in “social engineering” attacks. He understands that term to mean manipulating people to get personal information that you want and gaining unauthorized access to information by using computers, personal information, and services. One social engineering attack was against an unknowing neighbor. Using his computer skills he gained access to her personal email account. He accomplished this by intercepting electronic data from the wireless network containing her email address. Armed with her email account information, Applicant then visited the internet service provider’s (ISP) website and attempted to login to view her account. When he could not guess the neighbor’s password, he executed the “forgot password” function and wrote down the basic security challenge questions. In an attempt to learn the neighbor’s maiden name (to answer the security challenge question), Applicant called the neighbor and fraudulently represented that he was planning a high school reunion for her grandparents. During the conversation he learned the neighbor’s maiden name. He then again went to the ISP website and attempted to gain access to the neighbor’s email account. Once more, he was denied access even though he could answer the challenge question. Undeterred, Applicant continued this social engineering attack by calling the ISP’s customer service center and fraudulently representing to them that he was the neighbor’s husband and he demanded access to the account. He was given access after giving the service representative the correct challenge question answer.[4]

With access to the neighbor’s account, Applicant was able to view her email at will. He viewed her personal emails, address book, and accessed her monthly billing statements for her phone and internet use. Additionally, he changed the welcome header on her email account by stating that she had been hacked. He also sent out a false mass email to her friends and family describing a personal situation. On another occasion he hacked into the neighbor’s computer hard drive and imbedded an inappropriate picture into her start up folder. The result of his action caused the picture to load anytime she started her computer. He attempted to access her email account about two weeks later, but was denied access because the password was changed. Applicant then went to the neighbor’s house in person offering his services as a computer technician who could run a diagnostic test on her computer and troubleshoot any problems she was experiencing. She declined his services. At that time, Applicant did not tell her that he had hacked her system, nor has he ever disclosed that

[3] GE 3; Tr. at 29-30, 33-35, 44-48.

[4] GE 3; Tr. at 39-42.

information to her because he feared the legal repercussions that could follow. Applicant admitted to these actions.[5]

Also in 2005, Applicant hacked into a state Department of Transportation electronic road sign. The road sign is used to warn approaching motorists of upcoming hazards and display messages on the sign such as “warning road work ahead”. Applicant was able to access the message codes on the sign by calling the sign’s manufacturer and falsely representing that he was a construction worker who needed the codes. He was provided this information and used it to access the sign’s computer. He then changed the sign’s message on several occasions. One of the messages he put on the sign was “police ahead” to warn motorists of police cars using radar for speed enforcement. He put this message up several times. He also put joke messages on the sign. He admitted to these actions. He did this because it was challenging and he thought it was amusing to change the sign.[6]

Applicant met with government investigators on September 27, 2007 and February 3, 2009. During these interviews he disclosed his hacking activities. There is no evidence in the record about any investigative interview conducted on July 25, 2007, as alleged in SOR ¶ 1.c. The government also agreed that no evidence was present.[7]

Applicant testified that he had matured since his hacking activities. He pointed out that he was young when they occurred. He also pointed out that in his current position he is trusted by the company to indentify computer vulnerabilities for their clients and has not violated that trust. A coworker, who possesses a security clearance, testified for the Applicant. The coworker has known Applicant for three years and sees him at work on a daily basis. He believes Applicant engages in only the highest of conduct, believes he is reliable, and trusts him completely.[8]

## 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.

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

[5] GE 3, Tr. at 29-30, 33-35, 44-48.

[6] GE 2, 3; Tr. at 32-33.

[7] GE 2, 3; Tr. at 67-69.

[8] Tr. at 24-25, 58-63.

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 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 conditions are potentially applicable:

> (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
>
> (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.

Applicant's admitted hacking activities, including his premeditated acts of gaining access to his neighbor's private email communications and his deliberate actions to interfere with state highway safety signs, are cause for concern. Even though he ultimately disclosed this conduct to investigators, his actions created vulnerabilities that affected his personal standing. AG ¶ 16(e) applies to SOR ¶¶ 1a. - 1.b.

SOR ¶ 1.c (alleging Applicant made a false statement to investigators on July 25, 2007) is not factually supported by the evidence. There is no evidence in the record of there even being an interview on the date alleged. Moreover, in the two interviews that are in evidence, the Applicant did disclose his hacking activities affecting the neighbor and the road sign. AG ¶ 16(b) does not apply to SOR ¶ 1.c.

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 especially considered the following:

> (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; and
>
> (e) the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation or duress.

Applicant's hacking and social engineering attacks on his neighbor and on public safety are not minor events. These were serious acts that violated a person's privacy and affected public safety. Although Applicant's actions took place five years ago, given the deliberate and premeditative nature of his actions, I cannot conclude that the passage of time overcomes what he did. Applicant did not convince me that these types of action will not recur. AG ¶ 17(c) does not apply. Applicant was forthcoming in disclosing his actions to investigators thereby reducing his vulnerability to exploitation. However, he has never disclosed his hacking activities to the neighbor-victim because he still fears legal consequences. AG ¶ 17(e) does not apply.

### 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 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 conditions that could raise a security concern and may be disqualifying. The following disqualifying conditions are potentially applicable:

> (a) illegal or unauthorized entry into any information technology system or component thereof;
>
> (b) illegal or unauthorized modification, destruction, manipulation or denial of access to information, software, firmware, or hardware in an information technology system; and
>
> (c) use of any information technology system to gain unauthorized access to another system or to a compartmented area within the same system.

Applicant’s hacking activities in 2005, as fully described under Guideline E above, fall under the three disqualifying conditions above. AG ¶¶ 40(a) – (c) apply.

The guideline also includes conditions that could mitigate security concerns arising from personal conduct. I have considered all of the mitigating conditions under AG ¶ 41 and especially considered the following:

> (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;

For the same reasons that AG ¶ 17(c) did not apply to Applicant's conduct under Guideline E, nor does AG ¶ 40(a) apply under this guideline.

**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 have considered Applicant's age at the time he engaged in the hacking conduct and the passage of time since the acts. Additionally, I have considered his current work environment and the strong recommendation he received from a coworker regarding Applicant's reliability and trustworthiness. However, I also considered Applicant's deliberate and premeditated actions, including falsely representing himself as someone else on more than one occasion, using his computer skills to violate a person's privacy, and interfering with public safety. Applicant failed to provide sufficient evidence 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 E, Personal Conduct  and Guideline M, Use of Information Technology Systems.

## 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: | AGAINST APPLICANT |
| Subparagraphs 1.a-1.b: | Against Applicant |
| Subparagraphs 1.c: | For Applicant |
| Paragraph 2, Guideline M: | AGAINST APPLICANT |
| Subparagraph 2.a: | Against 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 eligibility for a security clearance. Eligibility for access to classified information is denied.

Robert E. Coacher
Administrative Judge