DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 08-10804
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Francisco Mendez Jr., Esquire, Department Counsel
For Applicant: *Pro se*

January 24, 2011

Decision

RIVERA, Juan J., Administrative Judge:

Applicant's immaturity led to his questionable behavior. He was forthcoming and candid during the security clearance process. He received training about ethical behavior and the handling of classified and proprietary information. He expressed sincere remorse for his past questionable behavior and understands that it could adversely impact on his ability to hold a security clearance. He has matured into a good husband and responsible employee. His questionable behavior is not recent, it is unlikely to recur, and it does not cast doubt on Applicant's current judgment, reliability, and trustworthiness. Applicant mitigated security concerns under Guidelines E and M.

Statement of the Case

Applicant submitted a security clearance application on June 3, 2008. After reviewing the results of the ensuing background investigation, adjudicators for the Defense Office of Hearings and Appeals (DOHA) were unable to make a preliminary

affirmative finding[1] that it is clearly consistent with the national interest to grant Applicant's request for a security clearance.

On May 18, 2010, DOHA issued Applicant a statement of reasons (SOR), which specified the basis for its decision – security concerns under Guideline E (Personal Conduct), and Guideline M (Use of Information Technology Systems) of the adjudicative guidelines (AG).[2]

On June 1, 2010, Applicant responded to the SOR allegations and requested a hearing before an administrative judge. The case was assigned to me on August 23, 2010, to determine whether a clearance should be granted or denied. DOHA issued a notice of hearing on September 16, 2010, and the hearing was convened as scheduled on October 1, 2010.

The Government offered exhibits (GE) 1 and 2, which were admitted without objection. Applicant testified, and he presented exhibits (AE) 1 through 9, which were admitted without objection. I left the record open for Applicant to supplement it, and he timely submitted AE 10. DOHA received the transcript of the hearing (Tr.) on October 9, 2010.

Procedural Issues

Applicant testified with the assistance of two outstanding interpreters certified by the Registry of Interpreters for the Deaf.

On Government's motion, and with Applicant's consent, I amended the SOR to include Applicant's middle name (Marc). (Tr. 13)

Applicant agreed to his hearing date 15 days in advance of his hearing. At hearing, he also waived his right to 15 days advanced notice of his hearing.

Findings of Fact

Applicant admitted SOR ¶¶ 1.a and 1.b, with explanations. He admitted and denied, in part, the factual allegations in the SOR ¶ 2.a, with explanations. His admissions are incorporated here as findings of fact. After a thorough review of the evidence of record, and having considered Applicant's demeanor and testimony, I make the following findings of fact.

[1] Required by Executive Order 10865, *Safeguarding Classified Information Within Industry,* dated February 20, 1960, as amended; and Department of Defense (DoD) Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (Directive), dated January 2, 1992, as revised.

[2] Adjudication of this case is controlled by the AGs, implemented by the DoD on September 1, 2006.

Applicant is a 28-year-old network security risk assessment and mitigation specialist working for a government contractor since March 2008. He received interim access to classified information at the secret level in May 2008. He seeks his security clearance eligibility to retain his position.

Applicant graduated from high school in 2000. Between 2000 and 2007, he attended several colleges off-and-on in different states. In 2007, he completed his bachelor's degree in business administration with a concentration in information technology (IT). He married his wife in July 2008. They have no children.

During a July 2008 interview with an Office of Personnel Management (OPM) investigator, Applicant disclosed that between 2005 and 2008, he frequently attempted to and entered private wireless networks without authorization to test his ability to penetrate the networks. While in college, he was playing with computers, experimenting with what he was learning, and testing security programs and his own abilities.

Applicant used commercially available, specialized computer programs to monitor Internet traffic and identify the networks Internet Protocol (IP) addresses or he would enter random IP addresses to attempt to access them. He sought out and gained access to unsecure or weakly secured networks. He testified that even though he was able to break into the networks, he never entered, modified, or accessed the systems. Nor did he share this information with anyone else. He averred he emailed the persons or companies about their deficient security systems hoping they would fix it.

Applicant mistakenly believed his actions were not illegal because he did not enter the subjects systems, nor did he access or manipulate any personal information. He claimed he only identified the "key" to entering the subjects' computer system and proceeded no further.

In 2007, he entered the secured network of a real estate company in Hong Kong, China. Applicant testified he informed the company of his access to its network and advised them that their security was faulty. He never received any acknowledgment of his emails to companies or people about their networks' deficiency. He does not recall how many networks he accessed. At some of his friends' requests, he would also access their networks to identify security deficiencies. Applicant disclosed his questionable behavior to one of his supervisors.

Applicant stopped his questionable behavior when he started working for his current employer in 2008. As a result of his job, he received training about IT ethics and the handling of classified and proprietary information. Applicant now understands that his questionable behavior was unethical and illegal. Moreover, he now understands that such behavior could adversely impact on his ability to hold a security clearance, to keep his current job, or to work in the IT field.

Applicant expressed sincere remorse for his past behavior. He has matured during the last three years. He is now married and holds a full-time position with a large

government contractor. He is busy at work and at home and he no longer has the time to experiment or play with computers. He is dedicated to his wife and his work. He is considered to be technically proficient, and a valuable employee with good performance.

Policies

The President of the United States has the authority to control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to have access to such information. *Department of the Navy v. Egan*, 484 U.S. 518, 527 (1988). The President has authorized the Secretary of Defense to grant eligibility for access to classified information "only upon a finding that it is clearly consistent with the national interest to do so." Exec. Or. 10865, *Safeguarding Classified Information within Industry* § 2 (Feb. 20, 1960), as amended. The U.S. Supreme Court has recognized the substantial discretion of the Executive Branch in regulating access to information pertaining to national security, emphasizing that "no one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988).

Eligibility for a security clearance is predicated upon the applicant meeting the criteria contained in the adjudicative guidelines. These AGs are not inflexible rules of law. Instead, recognizing the complexities of human behavior, these guidelines are applied in conjunction with an evaluation of the whole person. An administrative judge's adjudicative goal is a fair, impartial, and commonsense decision. An administrative judge must consider all available, reliable information about the person, past and present, favorable and unfavorable to reach his decision.

The Government reposes a high degree of trust and confidence in persons with access to classified information. This relationship transcends normal duty hours and endures throughout off-duty hours. Decisions include, by necessity, consideration of the possible risk that the applicant may deliberately or inadvertently fail to safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation of potential, rather than actual, risk of compromise of classified information. Clearance decisions must be "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." *See* Exec. Or. 10865 § 7. *See also* Executive Order 12968 (Aug. 2, 1995), Section 3. Thus, nothing in this Decision should be construed to suggest that I have based this decision, in whole or in part, on any expressed or implied determination about Applicant's allegiance, loyalty, or patriotism. It is merely an indication that the Applicant has not met the strict guidelines the President and the Secretary of Defense have established for issuing a clearance.

Initially, the Government must establish, by substantial evidence, conditions in the personal or professional history of the applicant that may disqualify the applicant from being eligible for access to classified information. The Government has the burden of establishing controverted facts alleged in the SOR. *See Egan*, 484 U.S. at 531.

"Substantial evidence" is "more than a scintilla but less than a preponderance." *See v. Washington Metro. Area Transit Auth.*, 36 F.3d 375, 380 (4th Cir. 1994). The guidelines presume a nexus or rational connection between proven conduct under any of the criteria listed and an applicant's security suitability. *See* ISCR Case No. 95-0611 at 2 (App. Bd. May 2, 1996); and ISCR Case 08-06605 at 3 (App. Bd. Feb. 4, 2010).

Once the Government establishes a disqualifying condition by substantial evidence, the burden shifts to the applicant to rebut, explain, extenuate, or mitigate the facts. Directive ¶ E3.1.15. An applicant "has the ultimate burden of demonstrating that it is clearly consistent with the national interest to grant or continue [his or her] security clearance." ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002). The burden of disproving a mitigating condition never shifts to the Government. *See* ISCR Case No. 02-31154 at 5 (App. Bd. Sep. 22, 2005). "[S]ecurity clearance determinations should err, if they must, on the side of denials." *Egan*, 484 U.S. at 531; *see* AG ¶ 2(b).

Analysis

Guideline E, Personal Conduct

AG ¶ 15 explains why personal conduct is a security concern stating:

> 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 facts and circumstances raising security clearance concerns under Guidelines E and M are the same. For the sake of brevity, they will be discussed here and incorporated by reference in the discussion of Guideline M.

Between 2005 and 2008, Applicant frequently broke into private wireless networks without authorization to test his ability to penetrate the networks. Although he was able to break into the networks, he never entered, modified, or accessed the private systems. Nor did he share this information with anyone else. He emailed the persons or companies' network systems he penetrated and informed them of their deficient security systems hoping they would fix it.

Applicant mistakenly believed his actions were not illegal because he did not enter the subjects' systems. He did not access or manipulate any personal information. He claimed he stopped when he identified the "key" to entering the subjects' computer systems. In 2007, he entered the secured network of a real estate company in Hong Kong, China. His actions trigger the applicability of the following disqualifying conditions:

AG ¶ 16(c): credible adverse information in several adjudicative 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; and

AG ¶ 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: . . .

(3) a pattern of dishonesty or rule violations.

AG ¶ 17 lists seven conditions that could potentially mitigate the personal conduct security concerns:

(a) the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts;

(b) the refusal or failure to cooperate, omission, or concealment was caused or significantly contributed to by improper or inadequate advice of authorized personnel or legal counsel advising or instructing the individual specifically concerning the security clearance process. Upon being made aware of the requirement to cooperate or provide the information, the individual cooperated fully and truthfully;

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

(d) the individual has acknowledged the behavior and obtained counseling to change the behavior or taken other positive steps to alleviate the stressors, circumstances, or factors that caused untrustworthy, unreliable, or other inappropriate behavior, and such behavior is unlikely to recur;

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

(f) the information was unsubstantiated or from a source of questionable reliability; and

(g) association with persons involved in criminal activity has ceased or occurs under circumstances that do not cast doubt upon the individual's reliability, trustworthiness, judgment, or willingness to comply with rules and regulations.

Applicant voluntarily disclosed his questionable behavior on his SCA, during his interview with an OPM investigator, and to one of his supervisors. The Government had no knowledge of his behavior before his disclosure. Since the start of his current job, he has received yearly training about his IT ethical responsibilities and in the proper handling of proprietary and classified information. In May 2008, he received an interim secret clearance. There is no evidence that he has compromised or caused others to compromise classified information, or that he has failed to follow his job's rules and regulations.

Most of Applicant's unauthorized intrusions into private networks occurred while he was attending college. He accessed the networks to test his ability to penetrate the networks. He was playing with computers, experimenting with what he was learning in college and testing security programs and his own abilities. He never entered, modified, or accessed the systems after breaking into the private networks security systems. Nor did he share this information with anyone else. He averred he emailed network's owners about their deficient security system hoping they would fix it. Applicant mistakenly believed his actions were not illegal because he did not enter the subjects' systems. He did not access or manipulate any personal information. He only identified the "key" to enter the subjects' computer systems and stopped there.

Applicant stopped his questionable behavior in 2008, when he started working for his current employer. He completed courses and received training about IT ethics and the handling of classified and proprietary information. He now clearly understands that his past questionable behavior was unethical and illegal. Moreover, he also understands that such behavior could adversely impact on his ability to hold a security clearance.

Applicant expressed sincere remorse for his past behavior. He is now a responsible husband. He is considered to be a good worker and a valuable employee. Applicant has matured during the last three years. He is dedicated to his wife and his work. He is considered to be technically proficient, valuable employee.

Guideline M, Use of Information Technology Systems

AG ¶ 39 articulates the security concern about the misuse 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.

Applicant's questionable behavior, as discussed under Guideline E, also raise security concerns under AG ¶ 40(a): "illegal or unauthorized entry into any information technology system or component thereof;" and AG ¶ 40(c): "use of any information technology system to gain unauthorized access to another system or to a compartmented area within the same system."

AG ¶ 41 provides three potentially applicable mitigating conditions to the use of information technology systems concern:

(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 supervisor.

For the same reasons discussed under the Guideline E mitigating conditions, incorporated here, I find that AG ¶ 41(a) applies. The circumstances in his life have changed and the misuse of his computer is not likely to recur. AG ¶¶ 41(b) and (c) are not applicable to Applicant's behavior because his misuse was not minor and his conduct was intentional.

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 relevant 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.

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. AG ¶ 2(c). I have incorporated my comments under Guidelines E and M in my whole-person analysis. Some of the factors in AG ¶ 2(c) were previously addressed under those guidelines, but some warrant additional comment.

Applicant's questionable behavior is primarily attributed to his immaturity as a college student. He voluntarily disclosed his questionable behavior in his 2008 SCA and was forthcoming and candid during the security clearance process and at his hearing. He stopped his questionable behavior in 2008, when he started working for his current employer. He received yearly training about ethical behavior and the handling of classified and proprietary information. He understands that his past questionable behavior was unethical and illegal. Moreover, he clearly understands that such behavior could adversely impact on his ability to hold a security clearance.

Applicant expressed sincere remorse for his past behavior. He is now a responsible husband. He has held his full-time job since March 2008, and he is considered to be a good worker and a valuable employee. Applicant has matured during the last three years. On balance, I find that Applicant's questionable behavior is not recent, it is unlikely to recur, and it does not cast doubt on Applicant's current judgment, reliability, and trustworthiness.

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
Subparagraphs 1.a and 1.:	For Applicant
Paragraph 2, Guideline M:	FOR APPLICANT
Subparagraph 2.a:	For Applicant

Conclusion

In light of all the circumstances presented by the record in this case, it is clearly consistent with the national interest to grant or continue eligibility for a security clearance for Applicant. Security clearance is granted.

_____

JUAN J. RIVERA
Administrative Judge