DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 10-04743
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Melvin A. Howry, Esq., Department Counsel
For Applicant: *Pro se*

August 22, 2011

Decision

LOUGHRAN, Edward W., Administrative Judge:

Applicant has mitigated use of information technology systems, drug involvement, and personal conduct security concerns. Eligibility for access to classified information is granted.

Statement of the Case

On February 10, 2011, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) to Applicant detailing security concerns under Guidelines M (use of information technology systems), H (drug involvement), and E (personal conduct). 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.

Applicant answered the SOR in writing on April 15, 2011, and elected to have the case decided on the written record in lieu of a hearing. Department Counsel submitted

the Government's written case on May 25, 2011. A complete copy of the file of relevant material (FORM) was provided to Applicant, who was afforded an opportunity to file objections and submit material to refute, extenuate, or mitigate the security concerns. Applicant received the FORM on June 7, 2011. As of August 2, 2011, he had not responded. The case was assigned to me on August 3, 2011. The Government exhibits included in the FORM are admitted.

Findings of Fact

Applicant is a 24-year-old software/systems engineer for a defense contractor. He is applying for a security clearance for the first time. His Questionnaire for National Security Positions (SF 86), submitted in October 2009, listed that he has worked for his current employer since August 2009, he has a bachelor's degree that was awarded in 2009, he has never been married, and he does not have children.[1]

Applicant has had an interest in computers and computer systems since he was a child. When he was in the seventh or eighth grade, he experimented with creating Trojan horses, a form of computer malware. There is no evidence that he ever transmitted the Trojan horses.[2]

In about June 2002, when he was 14 or 15 years old, Applicant created and operated a "botnet" program of about 30 computers and illegally accessed the computers, without their owners' knowledge or permission. A botnet is a group of related or unrelated computers that someone has gained control over. Applicant downloaded a program over the Internet for free. The program scans for vulnerable programs over the Internet. Applicant stated that he operated the botnet for experimental purposes. He never looked into the computers he accessed, and he did not alter them. He disabled the botnet after about two or three weeks.[3]

Applicant used to spend time at a Starbucks when he was in college. The store provided free wireless Internet access, but it was slow. The food shop next store had wireless Internet service, and the signal was accessible from the Starbucks. In about April 2009, Applicant's friend figured out that the food shop's password was the shop's phone number backwards. He provided the password to Applicant, and they both used it to access the Internet while they were at Starbucks. Applicant later learned that the food shop provided wireless Internet access for free.[4]

Other than the incidents discussed above, Applicant denied any other inappropriate information technology (IT) actions. He stated that he is now committed to securing and defending computer networks, and that he uses "all knowledge that [he

[1] Item 4.

[2] Items 3, 6.

[3] Items 3-7

[4] *Id.*

has] gained through [his] passion to strengthen and protect computer networks and [he is] an active member in the professional security community." He has obtained two computer security certifications. He has attended multiple computer security conferences. He participated as a member of his university's team in the National Cyber Defense Competition. Applicant's friends and co-workers are aware of the incidents addressed above. He listed his involvement with the botnet and his accessing the food store's wireless Internet when he submitted his SF 86 in October 2009. He volunteered the information about the Trojan horses when he responded to DOHA interrogatories in October 2010.[5]

Applicant smoked marijuana while he was in college. He estimated that between June 2007 and July 2009, he smoked marijuana about five times a week. He also experimented with other illegal drugs. He used cocaine on three occasions in 2007. He used psychedelic mushrooms on one occasion in 2007. He used the prescription drug Adderal without a prescription on one occasion in 2008. He purchased marijuana for his own use, and he also purchased Adderal on one occasion and ecstasy on one occasion. He did not use the ecstasy.[6]

Applicant listed his drug use on his October 2009 SF 86. He was interviewed by an investigator from the Office of Personnel Management (OPM) in November 2009. He fully discussed his drug use. He told the investigator that he stopped using marijuana in order to obtain a job with his current employer. He stated that he had no intention to use illegal drugs in the future. In his April 2011 response to the SOR, Applicant stated that he had not used illegal drugs since July 2009, before he started working for his current employer. He stated that he had never used illegal drugs during his professional career or while holding a security clearance. He reiterated that he does not intend to use illegal drugs in the future.[7]

Applicant submitted a letter from his lead engineer, a military service academy graduate with extensive experience in the military and as a defense contractor. He wrote that Applicant is "one of the top two or three performers [he had] ever met." He stated that Applicant is honest and forthright. He wrote that Applicant has received accolades and recognition for his outstanding job performance. He stated that Applicant "is not satisfied with his current level of professional competence and is continuing to pursue additional computer security certifications in order to gain even more job-related skills."[8]

[5] *Id.*

[6] *Id.*

[7] *Id.*

[8] Item 3.

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 to be 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, administrative judges apply the guidelines 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 the applicant or proven by Department Counsel." The applicant 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 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.

Section 7 of EO 10865 provides that adverse 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

The security concern for use of information technology systems is set out in AG ¶ 39:

> 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 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 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;
>
> (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.

Applicant's creation of the botnet and his access to the food shop's wireless Internet access establish all the above disqualifying conditions.

Applicant experimented with creating Trojan horses when he was in the seventh or eighth grade. There is no evidence that he ever transmitted the Trojan horses. That conduct, which occurred when Applicant was still in grade school, does not raise a security concern. SOR ¶ 1.a is concluded for Applicant.

Conditions that could mitigate the use of information technology systems security concerns are provided under AG ¶ 41. The following is potentially applicable:

(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.

The creation of the botnet was a serious violation of computer security, but it happened when Applicant was 14 or 15 years old. The use of the food store's wireless Internet was less serious, as the store provided free Internet access for its customers. Applicant's interest in IT from a young age led to the alleged conduct, but it also led to his current job as a software/systems engineer protecting systems. I find that his misuse of IT systems is unlikely to recur, and it does not cast doubt on his current reliability, trustworthiness, and good judgment. AG ¶ 41(a) is applicable.

Guideline H, Drug Involvement

The security concern for drug involvement is set out in AG ¶ 24:

Use of an illegal drug or misuse of a prescription drug can raise questions about an individual's reliability and trustworthiness, both because it may impair judgment and because it raises questions about a person's ability or willingness to comply with laws, rules, and regulations.

The guideline notes several conditions that could raise security concerns under AG ¶ 25. Two are potentially applicable in this case:

(a) any drug abuse;[9] and

(c) illegal drug possession, including cultivation, processing, manufacture, purchase, sale, or distribution; or possession of drug paraphernalia.

Applicant's drug possession and use are sufficient to raise AG ¶¶ 25(a) and 25(c) as disqualifying conditions.

AG ¶ 26 provides conditions that could mitigate security concerns. The following are potentially applicable:

(a) the behavior happened so long ago, was so infrequent, or happened under such circumstances that it is unlikely to recur or does not cast doubt on the individual's current reliability, trustworthiness, or good judgment; and

(b) a demonstrated intent not to abuse any drugs in the future, such as:

(1) disassociation from drug-using associates and contacts;

[9] Drug abuse is the illegal use of a drug or use of a legal drug in a manner that deviates from approved medical direction.

(2) changing or avoiding the environment where drugs were used;

(3) an appropriate period of abstinence;

(4) a signed statement of intent with automatic revocation of clearance for any violation.

Applicant used marijuana on a regular basis while he was in college. He also experimented with other illegal drugs in 2007 and 2008. He has not used any illegal drugs since he joined the workforce more than two years ago. He clearly and unequivocally committed to remaining drug-free. I find that he demonstrated an appropriate period of abstinence, and that illegal drug use is unlikely to recur. AG ¶¶ 26(a) and 26(b) are applicable.

Guideline E, Personal Conduct

The security concern 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.

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

> (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; and
>
> (e) personal conduct, or concealment of information about one's conduct, that creates a vulnerability to exploitation, manipulation, or duress, such as . . . engaging in activities which, if known, may affect the person's personal, professional, or community standing.

Applicant displayed questionable judgment and an unwillingness to comply with rules and regulations when he created the botnet, accessed the food shop's wireless Internet access, and became involved in illegal drugs. That conduct also created a vulnerability to exploitation, manipulation, and duress. AG ¶¶ 16(c) and 16(e) are applicable as disqualifying conditions.

AG ¶ 17 provides conditions that could mitigate security concerns. The following are potentially applicable:

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

Applicant has been open and honest about his misuse of IT systems and his illegal drug involvement, which reduces his vulnerability to exploitation, manipulation, and duress. AG ¶ 17(e) is applicable. AG ¶¶ 17(c) and 17(d) are also applicable under the same rationale discussed under Guidelines M and H.

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 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.

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

Applicant exhibited blatant disregard for the law in high school and college when he illegally accessed IT systems and used illegal drugs. He now has a job that he clearly loves and is very good at. He applies what he has learned to protect systems against unauthorized intrusions. I am convinced that he has put his inappropriate and illegal behavior behind him, and it will not recur.

Overall, the record evidence leaves me without questions or doubts about Applicant's eligibility and suitability for a security clearance. I conclude Applicant has mitigated use of information technology systems, drug involvement, and personal conduct security concerns.

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:	FOR APPLICANT
Subparagraphs 1.a-1.c:	For Applicant
Paragraph 2, Guideline H:	FOR APPLICANT
Subparagraphs 2.a-2.g:	For Applicant
Paragraph 3, Guideline E:	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.

_____
Edward W. Loughran
Administrative Judge