DATE: January 24, 2005

In Re:

SSN: ----------

Applicant for Security Clearance

ISCR Case No. 03-23474

DECISION OF ADMINISTRATIVE JUDGE

DARLENE LOKEY ANDERSON

APPEARANCES

FOR GOVERNMENT

Jennifer I. Campbell, Department Counsel

FOR APPLICANT

Robert Charles Wherley, Personal Representative

SYNOPSIS

Applicant's misuse of information technology by hacking into various computer systems without authority, his foreign influence, including foreign family ties, and his intentional falsification of his security clearance application concerning the extent of his marijuana use have not been mitigated. Clearance is denied.

STATEMENT OF THE CASE

On August 16, 2004, the Defense Office of Hearings and Appeals (DOHA), pursuant to Executive Order 10865 (as amended), and Department of Defense Directive 5220.6 (Directive), dated January 2, 1992, issued a Statement of Reasons (SOR) to the Applicant, which detailed the reasons why DOHA could not make the preliminary affirmative finding under the Directive that it is clearly consistent with the national interest to grant or continue a security clearance for the Applicant and recommended referral to an Administrative Judge to determine whether a clearance should be denied or revoked.

The Applicant responded to the SOR in writing on September 7, 2004, and requested a hearing before a DOHA Administrative Judge. This case was assigned to the undersigned on November 1, 2004. A notice of hearing was issued on November 10, 2004, scheduling the hearing for December 13, 2005. At the hearing the Government presented eleven exhibits. The Applicant called four witnesses and presented four exhibits. He also testified on his own behalf. The official transcript (Tr.) was received on December 28, 2004.

FINDINGS OF FACT

The following Findings of Fact are based on Applicant's Answer to the SOR, the exhibits and the testimony. The Applicant is 30 years of age and holds a Bachelors Degree in Computer Science. He is employed as a Software Engineer for a defense contractor. He seeks a security clearance in connection with his employment in the defense industry.

Paragraph 1 (Guideline M - Misuse of Information Technology Systems). The Government alleges in this paragraph that

the Applicant is ineligible for clearance because he has engaged in noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems that may raise security concerns about an individual's trustworthiness, willingness, and ability to properly protects classified systems, networks, and information.

From 1992 through 1998, the Applicant, while a college student, engaged in a variety of illegal activities involving the subversion of information technology systems. In each instance, the Applicant knew that his conduct was illegal. He indicates that it was not done with any criminal intent, but that he was simply curious. (Tr. p. 69). The Applicant found these activities to be intellectually challenging. The Applicant states that he is no longer involved in computer hacking, reading black market publications and he has not done so since 1998. (*See* Government Exhibit 2). He states that he has no intentions to ever engage in this conduct again.

In 1998, the Applicant while a student at a University hacked into the library catalog computer program of another University, and placed a test file with a particular statement on it into the second University's computer hard drive without authority. The Applicant did this in order to create a rivalry between the students and the system administrator at that college. The Applicant now realizes that this was an immature prank. (Tr. pp. 52 - 53).

In 1996 or 1997, the Applicant attempted to hack into the Department of Defense computer system on approximately four or five occasions. He explained that he saw the address for the Department of Defense in a black market magazine and he tried to log on. He states that he did not succeed. He explained that he simply wanted to see if the Department of Defense systems were reachable from the network at his University.

In 1998, the Applicant hacked into what he believed to be a national company's credit check computer terminal on five or six occasions using his personal computer. The Applicant claims that the information he received was not readable.

In September 1998, the Applicant changed the root password on his UNIX workstation at his place of employment without proper authority. The Applicant stated that he subverted the security measures on the system to change the password for productive reasons to stay on schedule and meet a deadline at work. The Applicant immediately informed the system administration group that he had administrative access and needed it to complete his work. He was then granted root privileges.

The Applicant has made at least $50.00 in fraudulent telephone calls using a "red box". The Applicant explained that a "red box" modifies the dialer to generate quarter tones so that the pay telephone thinks that it is receiving quarters, when in fact it is not.

The Applicant has attended various hacker group meetings and conferences in Los Angeles and San Francisco from 1996 until 1998. (Tr. p. 56). The meetings discussed computer security. The Applicant did not participate in any illegal activities during his attendance at the conferences or meetings. During this same period, the Applicant was reading black market publications that discuss, among other things, how to subvert different security systems.

Paragraph 2 (Guideline B - Foreign Influence). The Government alleges in this paragraph that the Applicant is ineligible for clearance because he has foreign contacts that could create the potential for foreign influence that could result in the compromise of classified information.

The Applicant is a naturalized American citizen. He has three uncles who are citizens of Egypt currently residing in Egypt. They have all completed military service in Egypt. The Applicant maintains monthly telephone contact with one uncle in Egypt, who is a University professor. His conversations with any of his uncles are limited because of the language barrier. They speak Arabic and no English. He speaks only English and very little Arabic. They are not affiliated in any way with the Egyptian Government.

In 1998, during his security clearance investigation, the Applicant stated that he would ask to be removed from any project that would be utilized in Egypt as he was loyal to his family members that reside in that region and would be concerned about their welfare. (*See* Government Exhibits 8 and 9). He explained that he simply answered the question honestly and did not realize that it would be interpreted as loyalty to another country. He also told the security investigation that he would continue to protect any information that he gained about the project and continue to follow all security regulations.

During the same security clearance investigation, a memorandum of the interview dated February 1999 indicates that the Applicant stated that he advised his references not to discuss information regarding his alcohol abuse, depression, computer hacking/phone switches and illegal drug activity with the Government investigator. The Applicant denies advising his references of such. *(See* Government Exhibit 8). The Applicant was denied access to Sensitive Compartmentalized Information on July 26, 1999. (*See* Government Exhibit 6 and 7).

Paragraph 2 (Guideline E - Personal Conduct). The Government alleges that the Applicant is ineligible for clearance because he engaged in conduct involving questionable judgment, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations could indicate that the person may not properly safeguard classified information.

The Applicant completed a security clearance application dated September 2, 1998, wherein he was required to indicate whether since the age of sixteen or in the last seven years, whichever is shorter, has he illegally used any illegal drugs. The Applicant answered, "YES", and listed that he used marijuana one time in December 1997, and again in October 1996. (*See* Question 27 of Government Exhibit 1). He failed to list that he had actually used marijuana more frequently between 1996 and January 1998.

The Applicant testified that he had no intention to falsify or provide inaccurate information to the Government. He testified that when he completed the application, he only remembered two occasions where he used marijuana, and he later remembered more. However, I do not find this explanation credible. The Applicant testified that he completed the security clearance questionnaire in September 1998, the very same year he admitted to using marijuana. It is difficult to understand how he could have forgotten that marijuana use. Based upon this, I believe that the Applicant intentionally concealed his marijuana use from the Government so that it would appear that he used it only in his distant past, when in fact he was either still using marijuana at the time he completed the security application or shortly before completing it. Accordingly, I find against the Applicant under Guideline E.

Mitigation.

Four witnesses who know the Applicant very well, including his manager, coworkers and friends, testified that they consider the Applicant to be extremely honest, trustworthy and reliable.

Letters of recommendation submitted on the Applicant's behalf indicate that he is considered to be a person of high integrity. He is professional, stable, trustworthy and capable. It is believed that he has followed all of the security regulations and obeyed all system policies that are in place at his place of employment. (*See* Applicant's Exhibit A).

The Applicant states that he is married, has two children and is more mature than he was in college.

POLICIES

Security clearance decisions are not made in a vacuum. Accordingly, the Department of Defense, in Enclosure 2 of the 1992 Directive sets forth policy factors and conditions that could raise or mitigate a security concern; which must be given binding consideration in making security clearance determinations. These factors should be followed in every case according to the pertinent criterion. However, the conditions are neither automatically determinative of the decision in any case, nor can they supersede the Administrative Judge's reliance on her own common sense. Because each security clearance case presents its own unique facts and circumstances, it cannot be assumed that these factors exhaust the realm of human experience, or apply equally in every case. Based on the Findings of Fact set forth above, the factors most applicable to the evaluation of this case are:

Guideline M (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 trustworthiness, willingness, and ability to properly protect classified systems, networks, and information. Information Technology Systems include all related equipment used for the communication, transmission, processing, manipulation, and storage of classified or sensitive information.

Conditions that could raise a security concern and may be disqualifying:

1. Illegal or authorized entry into any information technology system;

2. Illegal or unauthorized modification, destruction, manipulation, or denial of access to information residing on an information technology system.

Conditions that could mitigate security concerns:

None.

Guideline B (Foreign Influence)

A security risk may exist when an individual's immediate family, including cohabitants, and other persons to whom he or she may be bound by affection, influence, or obligation are: (1) not citizens of the United States or (2) may be subject to duress. These situations could create the potential for foreign influence that could result in the compromise of classified information. Contacts with citizens of other countries or financial interests in other countries are also relevant to security determinations if they make an individual potentially vulnerable to coercion, exploitation, or pressure.

Condition that could raise a security concern:

1. An immediate family member, or person to whom the individual has close ties of affection or obligation, is a citizen of, or resident or present in, a foreign country;

Condition that could mitigate security concerns:

None.

Guideline E (Personal Conduct)

Conduct involving questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations could indicate that the person may not properly safeguard classified information.

Conditions that could raise a security concern:

2. The deliberate omission, concealment, or falsification of relevant and material facts from any personnel security questionnaire, personal history statement, or similar form used to conduct investigations, determine employment qualifications, award benefits or statute, determine security clearance eligibility or trustworthiness, or award fiduciary responsibilities;

5. A pattern of dishonesty or rule violations.

Conditions that could mitigate security concerns:

None.

In addition, as set forth in Enclosure 2 of the Directive at pages 16-17, in evaluating the relevance of an individual's conduct, the Administrative Judge should consider the following general factors:

a. The nature and seriousness of the conduct and surrounding circumstances

b. The circumstances surrounding the conduct, to include knowledgeable participation

c. The frequency and recency of the conduct

d. The individual's age and maturity at the time of the conduct

e. The voluntariness of participation

f. The presence or absence of rehabilitation and other pertinent behavior changes

g. The motivation for the conduct

h. The potential for pressure, coercion, exploitation or duress

i. The likelihood of continuation or recurrence.

The eligibility criteria established in the DoD Directive identify personal characteristics and conduct which are reasonably related to the ultimate question, posed in Section 2 of Executive Order 10865, of whether it is "clearly consistent with the national interest" to grant an Applicant's request for access to classified information.

The DoD Directive states, "The adjudicative process is an examination of a sufficient period of a person's life to make an affirmative determination that the person is eligible for a security clearance. Eligibility for access to classified information is predicted upon the individual meeting these personnel security guidelines. The adjudicative process is the careful weighing of a number of variables known as the whole person concept. Available, reliable information about the person, past and present, favorable and unfavorable should be considered in reaching a determination. The Administrative Judge can draw only those inferences or conclusions that have reasonable and logical basis in the evidence of record. The Judge cannot draw inferences or conclusions based on evidence which is speculative or conjectural in nature. Finally, as emphasized by President Eisenhower in Executive Order 10865, "Any determination under this order . . . shall be a determination in terms of the national interest and shall in no sense be a determination as to the loyalty of the Applicant concerned."

The Government must make out a case under Guideline B (foreign influence) and Guideline E (Personal Conduct) that establishes doubt about a person's judgment, reliability and trustworthiness. While a rational connection, or nexus, must be shown between Applicant's adverse conduct and his ability to effectively safeguard classified information, with respect to sufficiency of proof of a rational connection, objective or direct evidence is not required.

Then, the Applicant must remove that doubt with substantial evidence in refutation, explanation, mitigation or extenuation, which demonstrates that the past adverse conduct, is unlikely to be repeated, and that the Applicant presently qualifies for a security clearance.

An individual who demonstrates that he has foreign connections may be prone to provide information or make decisions that are harmful to the interests of the United States. The mere possession of a foreign passport raises legitimate questions as to whether the Applicant can be counted upon to place the interests of the United States paramount to that of another nation. The Government must be able to place a high degree of confidence in a security clearance holder to abide by all security rules and regulations, at all times and in all places.

CONCLUSIONS

Having considered the evidence in light of the appropriate legal standards and factors, and having assessed the Applicant's credibility based on the record, this Administrative Judge concludes that the Government has established its case as to all allegations in the SOR, and that Applicant's misuse of information technology, foreign influence personal conduct and have a direct and negative impact on his suitability for access to classified information.

The Applicant is a naturalized born United States citizen who has three uncles who are citizens of and reside in Egypt. The Applicant has very little contact with his uncles in Egypt. None of his uncles are connected with the Egyptian Government. Under most circumstances, mitigating condition 1 would apply. However, the Applicant during an interview with the Defense Security Service the Applicant indicated that although he is a loyal United States citizen he would ask to be removed from a United States project that would be utilized in Egypt because of his loyalty to his family members that reside in Egypt and his concern for their welfare. The Applicant has not resolved this concern with any current evidence. Under these circumstances, I find that the Applicant is vulnerable to foreign influence. Based on

the foregoing, this raises a security concern and Guideline B is found against the Applicant.

As previously discussed, I find that the Applicant intentionally falsified his security clearance application of 1998, in response to question 27 concerning the extent of his use of marijuana. Even though seven years has past since he completed the application, his refusal to admit that he lied makes it impossible to mitigate. The Applicant has shown questionable judgment, untrustworthiness and lacks the candor and honesty required to access the national secrets. Accordingly, I find against the Applicant under Guideline E.

The Applicant's misuse of information technology while in college from 1992 through 1998 shows a pattern of questionable judgment and is another example of his untrustworthiness. Although he was young and immature at the time he engaged in the conduct, I still question his ability to understand the security responsibilities and to fulfill them. His interest in subverting security systems, hacking into unauthorized computer systems, reading black market publications and attending conferences and meetings on security systems for the purpose of undermining their process demonstrates extremely poor judgment as well as a criminal mentality. This illegal conduct took place over the course of a six year period. This illegal conduct is the very conduct that the Department of Defense is seeking to protect against. Although the conduct occurred slightly over seven years ago, hacking by its very nature is a significant offense requiring careful scrutiny. Individuals with this particular knowledge must be examined closely. In fact, in this case, the Applicant tried to hack into the Department of Defenses computer system. Despite knowing the conduct was illegal, his intellectual stimulation and curiosity took priority. Furthermore, although he believes that his conduct did not hinder, delay or harm the computer systems that he broke into, he really does not know the consequences that his actions may have had. Disqualifying conditions *1. Illegal or authorized entry into any information technology system,* and *2. Illegal or unauthorized modification, destruction, manipulation, or denial of access to information residing on an information technology system* apply. None of the mitigating factors apply. Although the conduct was not recent, it was significant, intentional, unauthorized, not isolated and he made no good faith effort to correct the situations. More time is needed to determine that his curiosity will not prevail when it comes to hacking. In addition, based upon his credibility in the past, I cannot find that the Applicant can be trusted with the national secrets at this time. Accordingly, I find against him under Guideline M.

Considering all the evidence, the Applicant has not met the mitigating conditions of Guideline M of the adjudicative guidelines set forth in Enclosure 2 of the Directive. Accordingly, he has not met his ultimate burden of persuasion under Guidelines M, B and E.

FORMAL FINDINGS

Formal Findings For or Against the Applicant on the allegations in the SOR, as required by Paragraph 25 of Enclosure 3 of the Directive are:

Paragraph 1: Against the Applicant.

Subparas. 1.a.: Against the Applicant

1.b.: Against the Applicant 1.c.: Against the Applicant

1.d.: Against the Applicant

1.e.: Against the Applicant

1.f.: Against the Applicant

Paragraph 2: Against the Applicant.

Subparas. 2.a.: Against the Applicant

2.b.: Against the Applicant

2.c.: Against the Applicant

Paragraph 3: Against the Applicant.

Subparas. 3.a.: Against the Applicant

3.b.: Against the Applicant 3.c.: Against the Applicant

3.d.: Against the Applicant 3.e.: Against the Applicant

DECISION

In light of the circumstances presented by the record in this case, it is not clearly consistent with the national interests to grant or continue a security clearance for the Applicant.

Darlene Lokey Anderson

Administrative Judge