DATE: September 16, 2002

In Re:

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

Applicant for Security Clearance

ISCR Case No. 01-04172

DECISION OF ADMINISTRATIVE JUDGE

CLAUDE R. HEINY

APPEARANCES

FOR GOVERNMENT

Kathryn D. MacKinnon, Department Counsel

FOR APPLICANT

Sheldon I. Cohen

SYNOPSIS

While a computer science major in school and in his job following school, the Applicant was alleged to have acted inappropriately in a number of computer related incidents. The incidents fail to rise to the level of security concern under Guideline E (Personal Conduct) or misuse of an informational technology system under Guideline M. Clearance is granted.

STATEMENT OF THE CASE

On October 24, 2001, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) to Applicant, stating that DOHA could not make the preliminary affirmative finding[(1)] it is clearly consistent with the national interest to grant or continue a security clearance for Applicant. On December 6, 2001, the Applicant answered the SOR and requested a hearing. The case was assigned to me on February 6, 2002. A Notice of Hearing was issued on February 8, 2002, scheduling the hearing for March 4, 2002. For good cause, an Amended Notice of Hearing was issued on February 21, 2002 changing the hearing date which was held on April 2, 2002.

The Government's case consisted of eleven exhibits[(2)] (Gov Ex). The Applicant relied on his own testimony, four additional witnesses, and eleven exhibits (App Ex). The transcript (tr.) of the hearing was received on April 16, 2002.

FINDINGS OF FACT

The SOR alleges personal conduct (Guideline E) and noncompliance with rules, procedures, guidelines, or regulations pertaining to information technology systems (Guideline M). The Applicant denies the allegations.

The Applicant is 27-years-old, has worked for a defense contractor since June 1998, and is seeking to obtain a security clearance.

In 1987 or 1988, the Applicant's father came to the US from Egypt in search of a better life with more opportunity and freedom. The Applicant's family suffered from religious persecution in Egypt (Gov Ex 3, p 2). His father was in the US seven or eight years securing employment, before sending for his family. In 1989, at age 13, the Applicant came to the US. English is a second language to the Applicant, prior to his arrival in the US, he spoke little English. In 1993, the Applicant, his mother, and sister became US citizens. His father had become a US citizen earlier. In August 1994, the Applicant started his studies at a university where he graduated with high distinction honors (App Ex E), a 3.744 GPA (tr 278), and no disciplinary problems (tr 279). He is currently enrolled in a Master's program at the same university.

In 1995, the university published a policy (Gov Ex 8, 10, 11) on computer use. In 1997, the policy was restated (Gov Ex 5) to include reference to the university web site. It is uncertain if the policy was published on the web, but efforts were made to ensure all computer users were aware of the policy (tr 121). The Applicant was never formally or informally accused of violating the university computer policy. No disciplinary action was ever taken against the Applicant by the university. (App Ex D) The policy included using university computer resources consistent with the stated priorities, not allowing anyone to use one's account for an illegitimate purpose, honoring the privacy of other users, not impersonating others, and not using computer resources to violate other policies or laws. At some time, not further disclosed in the record, the university's computer policies would appear when users logged onto the system (Gov Ex 6). The university also has an end user computer security manual. It is unsure from the record how widely distributed this manual is or if the Applicant ever saw it.

Mr. A is the system administrator for Information Technology (IT) for the university's four libraries and is in charge of controlling the web server and administration of the IT system (tr. 53). Mr. A controls several hundred personal computers (PCs) used by the library staff and 200-300 PCs used by students. In 1997, Mr. A. hired the Applicant as a student worker and for one and a half year to two years with daily supervision of the Applicant. Mr. A found the Applicant to be reliable and very trustworthy. Because of the Applicant's knowledge, reliability, and trustworthiness, he was give root access[(3)] on the computer system, which is another name for superuser (tr 60). As a super user on the UNIX system, the Applicant had privileges to do anything on the system including changing files, adding or deleting users, and altering the systems configuration. To Mr. A's knowledge, the Applicant never abused his privileges.

University professors would put articles on an electronic reserve to be accessed by students. Students would access the material by using their passwords. University policy prohibits generic accounts and requires each account to be assigned to a particular student. Mr. A asked the Applicant to automate the log in system to determine if requests were being made by authorized users. (App Ex J) The prior system required a manual check to be made on each request. The Applicant also worked on the linking of the university's computers. In 1997, in testing the computer program he was developing, the Applicant used a "proxy[(4)]" to enter information into the university computer system. At the time, the Applicant was working on the team that maintained the university's web server.

In his sworn statement (Gov Ex 2) the Applicant described this as writing a proxy to enter an individual's personal data in the university computer system and accessed his own personal information. He then attempted to enter "dummy" numbers to see what resulted. In his statement he incorrectly defined proxy as a way to fake a password to gain access to an individual's information.

The Applicant's sister was also enrolled at the same university. The Applicant used a FIND program to determine if his sister was logged onto the university computer so he could contact her. The university e-mail system had 22,000 accounts which supported approximately 150 users at one time. A FIND program is one of a hundred utility programs pre-installed on PCs, a standard tool on PCs, and used to perform a simple task. Any user can use a FIND program which does not allow access into restricted files. Such a program cannot break into a computer. In his sworn statement (Gov Ex 2) he incorrectly describes using the FIND utility program as "the only time I ever attempted to damage a computer program."

In the Fall of 1997, on the first day of school, the Applicant logged onto the system using his correct identification and started a FIND program. The Applicant forgot to include a delay command in the FIND program which thereby created an endless loop. This error caused the program to use a significant amount of the computer's capability and slowed the system. When the system administrator noted the system slow down, he checked the current jobs listed by resources being consumed and noted the Applicant's program was consuming 45% of the system resources. When the system administrator noted the Applicant's application was high on the list, he contacted the Applicant by email and told him to

end the application. Shortly thereafter the administrator came to the Applicant's office and again told the Applicant to stop using the program and not do it again. The problem was caused by the Applicant's insufficient knowledge concerning the effect of linking commands. When the Applicant wrote the program he was not a sophisticated programer and had inadvertently created an endless loop by failing to include a delay or sleep command. (App Ex K) This was a typical beginner's mistaken (tr 234). The Applicant had no intent to damage the system and was not attempting to break into the system or manipulate the system. Other than this error, the applicant has never been told he had ever done anything wrong related to his use of computers. Mr. A. stated the Applicant had not acted improperly when the Applicant ran a FIND or "finger[(5)]" program.

In 1996, while a student, the Applicant wrote a program using a token[(6)] to test the system. The Applicant accessed a web page and entered his personal information on that page before modifying the token portion of the uniform resource locator (URL) (App Ex I, tr 71). He modified the token portion of the URL expecting to receive an error message, which was received. He was experimenting with the system which he had helped to develop. He was not attempting to gain access to another's information. In a signed, sworn statement dated August 1999 (Gov Ex 2) the Applicant described this as playing with a token without gaining access, to show the university personnel that he had attempted to gain access to the system.

In 1996, the Applicant had an account on a friend's computer system and had authority to access his friend's computer. The system was new to both of them and they experimented to determine how the system worked. In testing the system, the Applicant typed in garbage to determine if the system would accept the data. He was simply doing his job. He was curious about the operating system and experimenting. The Applicant never broke into nor gained access to his friend's system. In a signed, sworn statement(Gov Ex 2), the Applicant described this event as trying to connect with his friend's computer about ten times, when his friend "caught" him. The Applicant states there was no attempt to cause harm or destroy.

The Applicant worked for the university computer information system(CIS) from the Fall of 1995 into 1996, when he quit the job when his relationship with supervisors and coworkers was strained. The Applicant acknowledged he was young, had a bad attitude problem (tr 399), was disrespectful to management, and had a personality conflict with coworkers, but the main reason for leaving was the job required him to sit alone for eight hours per day. In his sworn statement (Gov Ex 2) he incorrectly states he was fired from the job. He put a message on a machine, which the system administrator did not like. After leaving the CIS, the Applicant would periodically attempt to log onto the system using his name or using a "funny name" just to see if he had access. He did this simply to get the employer's attention. He was never able to gain access to the system. (Gov Ex 2) He last attempted to log onto the system in November 1998.

Mr. B. knew the Applicant as a former co-worker when they shared an office together for several years. While Mr. B. was on vacation, the Applicant used Mr. B.'s computer to install a chess game. Individuals routinely installed personal software on the company's computers (tr 176). At the time of the incident, the Applicant had unlimited root access to the computer system (tr 340). Although Mr. B. did not authorize the Applicant to use the computer in his office, it was common in the company for individuals to use any vacant computer. Users would use each other's computers (tr 179). Today, the company provides everyone with their own computer, but at the time in question there were not enough computers for everyone to have their own machine so anyone could use any computer. At the time, everyone left their computers up and running (tr 170). When the Applicant used the computer, he viewed some of his co-worker's personal information concerning rental car information because Mr. B. had failed to lock the screen with a screen saver password before leaving on vacation. r. B. believes the Applicant to be honest to a fault (tr 171), that the Applicant states what is on his mind without considering whether or not it is wise or diplomatic. The Applicant sometimes lacks tact, but is diligent, trustworthy, reliable, and never devious (tr 172). While working for the company, the Applicant was never criticized or punished for misuse of computers. The company had a policy, process, and procedure system (Gov Ex 9) which addressed business conduct and use of company resources.

Mr. C., a coworker, believes the Applicant to be honest, open, enthusiastic, not bashful, shy or lazy, (tr 197) and if there is something on the Applicant's mind, the Applicant brings it out in the open. Mr. C. finds the Applicant to be an excellent communicator in English when he is calm, when excited he does not always make himself clearly understood. At those times, Mr. C. tells the Applicant to slow down, take a breath, think about what he wants to say, and start over (tr 241). Mr. C. believes any misunderstandings are caused by the Applicant's nervousness, his excitement, and his

desire to be totally honest, and the Applicant's failure to communicate accurately (tr 241). Mr. C. believes the Applicant to be fully honest.

The Applicant has never downloaded a password breaking, Trojan horse, or "cracking" program (Gov Ex 4, p 1, tr 324). A "cracker" attempts to breaks into other computer systems (tr 133). The Applicant did spend time experimenting with different systems and programs simply to learn more about the systems. Although the term computer "hacker" has taken on a malicious connotation the term originally meant a user who plays around with or experimented with codes, programs, or systems (134). The Applicant has never broken into a system or computer with or without permission (Gov Ex 4, p 1).

In May 1999, the Applicant made a signed, sworn statement (Gov Ex 4) to a Special Agent of the Defense Security Service (DSS) stating he had deliberately falsified material facts when he stated he had never broken into a computer system with or without permission.

While in high school, the Applicant did volunteer work with senior citizens and handicapped children. The Applicant is very active in his church, (App Ex F) is a deacon (tr 291), and has established a web site (App Ex G) and worked every day for six months translating a book on the life of a Coptic Orthodox Pope from Arabic to English. He is assisted by his sister, because her English is better than his for he does not understand and fails to grasp all of the nuances of the English language. He attends Bible study twice a week and volunteers at a local hospital. (App Ex H, tr 289)

POLICIES

The Adjudicative Guidelines in the Directive are not a set of inflexible rules of procedure. Instead, they are to be applied by Administrative Judges on a case-by-case basis with an eye toward making determinations that are clearly consistent with the interests of national security. In making overall common sense determinations, Administrative Judges must consider, assess, and analyze the evidence of record, both favorable and unfavorable, not only with respect to the relevant Adjudicative Guidelines, but in the context of factors set forth in section E 2.2.1. of the Directive as well. In that vein, the government not only has the burden of proving any controverted fact(s) alleged in the SOR, it must also demonstrate the facts proven have a nexus to an Applicant's lack of security worthiness.

The adjudication process is based on the whole person concept. All available, reliable information about the person, past and present, is to be taken into account in reaching a decision as to whether a person is an acceptable security risk. Although the presence or absence of a particular condition for or against clearance is not determinative, the specific adjudicative guidelines should be followed whenever a case can be measured against this policy guidance.

Considering the evidence as a whole, this Administrative Judge finds the following adjudicative guidelines to be most pertinent to this case:

Personal Conduct (Guideline E) The Concern: 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. The following will normally result in an unfavorable clearance action or administrative termination of further processing for clearance eligibility:

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

None Apply.

Misuse of Information Technology Systems (Guideline M) The Concern: 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 include:

None Apply.

BURDEN OF PROOF

Initially, the Government has the burden of proving any controverted fact(s) alleged in the Statement of Reasons. If the Government meets that burden, the burden of persuasion then shifts to the Applicant who must remove that doubt and establish his security suitability with substantial evidence in explanation, mitigation, extenuation, or refutation, sufficient to demonstrate that despite the existence of guideline conduct, it is clearly consistent with the national interest to grant or continue his security clearance.

A person who seeks access to classified information enters into a fiduciary relationship with the Government predicated upon trust and confidence. Where the facts proven by the Government raise doubts about an applicant's judgment, reliability or trustworthiness, the applicant has a heavy burden of persuasion to demonstrate that he is nonetheless security worthy. As noted by the United States Supreme Court in *Department of Navy v. Egan*, 484 U.S. 518, 531 (1988), "the clearly consistent standard indicates that security clearance determinations should err, if they must, on the side of denials." As this Administrative Judge understands the Court's rationale, doubts are to be resolved against the applicant.

CONCLUSIONS

Under Guideline E, the security eligibility of an applicant is placed into question when the Applicant is involved in 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. The Applicant's conduct was not a violation of the personal conduct guideline.

In 1996, while a student, the Applicant wrote a program using a token to test the system. He used the token expecting to receive an error message, which he received. He was experimenting with the system which he had helped to develop. He was not attempting to gain access to others' information. The Applicant was simply testing the system and this was not an illegal or unauthorized entry into an IT system. None of the Disqualifying Conditions (DC) apply to this. DC 1 [(7)], does not apply because the Applicant was authorized to test the system. I find for the Applicant as to SOR subparagraph 1.a.

In 1997, the Applicant was hired as a student worker. Because of the Applicant's knowledge, reliability, and trustworthiness, he was give root access on the computer system. As a super user on the UNIX system, the Applicant had privileges to do anything on the system including changing files, adding or deleting users, and altering the systems configuration. The Applicant also worked on the linking of the university's computers and was working on the team that maintained the university's web server. In 1997, in testing the computer program he was developing, the Applicant used a "proxy" to enter information into the university computer system which is a normal way to check to see if the program is functioning properly.

In his August 1999-sworn statement the Applicant described using the proxy to see what would happen. He incorrectly defined proxy as a way to fake a password to gain access to an individual's information. The Applicant did use a proxy, however it was not a way to fake a password. The Applicant made a number of statements in his sworn statement indicating his had acted inappropriately. The Applicant had not acted inappropriately but made these misstatements due to his command of the English language. English is a second language to the Applicant. Until age 12 the Applicant did not use English. Even now the nuances of English often escape him. Coworkers state the Applicant is an excellent communicator in English when he is calm, but when the Applicant becomes excited he does not always make himself clearly understood. When excited coworkers tell the Applicant to slow down, take a breath, think about what he wants to say, and start again.

Misstatements and misunderstandings are caused by the Applicant's nervousness, his excitement, his desire to be totally honest, his lack of knowledge of the nuances of English, which resulted in the Applicant's failure to communicate accurately. None of the Disqualifying Conditions apply to this. I find for the Applicant as to SOR subparagraph 1.b.

In 1997, the Applicant ran a FIND program, which is a utility program found on most computers. In his sworn statement

the Applicant incorrectly describes using the FIND utility program as "the only time I ever attempted to damage a computer program." Using such a utility program does not damage a computer. The Applicant never installed the FIND program for it came pre installed on the computer. There was no intent to damage the system nor was there an attempt to break into the system or manipulate the system. None of the Disqualifying Conditions apply to this. I find for the Applicant as to SOR subparagraph 1.c.

In 1996, the Applicant had an account on a friend's computer system and had authority to access a friend's computer. The system was new and both of them were experimenting to determine how the system worked and it capacities. Being curious about the operating system and experimenting the Applicant attempted to contact his friend's computer. Although the Applicant described this as trying to connect with his friend's computer when he got "caught," he did nothing wrong. There was no attempt to cause harm or destroy. None of the Disqualifying Conditions apply to this. Guideline M, DC 1. states an illegal or unauthorized entry into any information technology system. There is no showing the Applicant actually entered his friend's computer. Guideline M, does not address "attempted entry" into an IT system. I find for the Applicant as to SOR subparagraph 1.d.

While working for a defense contractor, the Applicant put a chess game on a coworker's computer. Although the coworker had not authorized the Applicant to do this, it was common in the company for individuals to use any vacant computer and individuals routinely installed personal software on the company's computers. At the time, everyone left their computers up and running and users would use each other's computers. When he put the game on his coworker's computer, the Applicant inadvertently saw some of his coworker's personal information. The Applicant was not looking for private information for he had unlimited root access to the entire computer system and could have viewed private information if he chose to do so, but never did. The viewing of the personal information was an inadvertent act. The Applicant was never criticized or punished for misuse of computers while at the company or at any time. None of the Disqualifying Conditions apply to this. I find for the Applicant as to SOR subparagraph 1.e.

In the Fall of 1997, on the first day of fall classes, the Applicant logged onto the system using his correct identification and started a FIND program so he could contact his sister. In writing the program, the Applicant forgot to include a sleep or delay command which, thereby, created an endless loop. This error caused the program to use a significant amount of the computer's capability and slowed the system. When told by the system administrator to end the program he did. The problem was caused by the Applicant's insufficient knowledge concerning the effect of linking commands which was a typical beginner's mistaken. There was no intent to damage the system nor was it an attempt to break into the system or manipulate the system. None of the Disqualifying Conditions apply to this. I find for the Applicant as to SOR subparagraph 1.f.

The Applicant's May 1999 statement that he had never broken into a system or computer with or without permission was a true statement. None of the Disqualifying Conditions apply to this. I find for the Applicant as to SOR subparagraph 1.g.

Under guideline M, Misuse of Information Technology Systems, the security eligibility of an applicant is placed into question when the Applicant is involved in 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. The Applicant's conduct did not violate any university rule, procedure, guideline, or regulation.

The university had a policy regarding computer use by its employees and students, which was revised from time to time (Gov Exs 5, 6, 7, 8, 10, 11). As a computer student the Applicant did experiment, examine, test, and tried out new things with the university's computers. In 1997, Mr. A, the system administrator for the university's four libraries web servers and administration of the IT system hired the Applicant as a student worker and had daily supervision over the Applicant for one and a half year. Mr. A. believes the Applicant to be reliable, trustworthy, knowledgeable, and reliable, and trustworthiness, and gave the Applicant root access on the computer system. As such the Applicant had privileges to do anything on the system including changing files, adding or deleting users, and altering the systems configuration. In making an automated log in system, the Applicant used proxies and tokens to test the system. Additionally, the Applicant experimented with the systems to learn about their capabilities, limitations, and how they functioned. None of the conduct alleged violates the university's computer use policy.

The university has never taken disciplinary action against the Applicant for any reason. The Applicant graduated with high distinction honors and is currently enrolled in a Master's program at the same university. Since a violation of the university's computer has not been proved, none of the disqualifying factors apply. There was no illegal or unauthorized entry into any information technology system (DC 1), no illegal or unauthorized modification, destruction, manipulation, or denial of access to information residing on an information technology system (DC 2), nor was there an introduction of hardware, software or media into any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations (DC 4).

Even if the Applicant's actions could be characterized as a violation of the rules, Mitigating

Factors 1 and 2 would apply. The last alleged violation occurred in 1997, which is five years ago, which means MC 1, the misuse was not recent, would be applicable. Additionally, MC 2 would apply because the Applicant's actions were unintentional or inadvertent.

In reaching my conclusions I have also considered: the nature, extent, and seriousness of the conduct; the Applicant's age and maturity at the time of the conduct; the circumstances surrounding the conduct; the Applicant's voluntary and knowledgeable participation; the motivation for the conduct; the frequency and recency of the conduct; presence or absence of rehabilitation; potential for pressure, coercion, exploitation, or duress; and the probability that the circumstance or conduct will continue or recur in the future.

FORMAL FINDINGS

Formal Findings as required by Section 3., Paragraph 7., of Enclosure 1 of the Directive are hereby rendered as follows:

Paragraph 1 Personal Conduct (Guideline E:) FOR THE APPLICANT

Subparagraph 1.a.: For the Applicant

Subparagraph 1.b.: For the Applicant

Subparagraph 1.c.: For the Applicant

Subparagraph 1.d.: For the Applicant

Subparagraph 1.e.: For the Applicant

Subparagraph 1.f.: For the Applicant

Subparagraph 1.g.: For the Applicant

Paragraph 2 Misuse of Information

Technology Systems (Guideline M): FOR THE APPLICANT

Subparagraph 2.a.: For the Applicant

DECISION

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 a security clearance for the Applicant.

Claude R. Heiny

Administrative Judge

1. Required by Executive Order 10865, as amended and Department of Defense Directive 5220.6 (Directive), dated January 2, 1992 as amended.

2. Gov Exs. 10 and 11 were admitted over the objection by Applicant's counsel.

3. No other user has more power or control over the system than a person who has root access (tr 115). Such users are trusted individuals since that have the ability to can bypass all security on the system.

4. A proxy takes information provided in one form and properly translates it to the format of another database. The proxy is a bridge or channel to pass information. It is a medium to transfer data between two pieces of code. The use of a proxy is a normal way to check to see if the program is functioning properly.

5. The purpose of a "finger" program is to determine what other users are on-line at a particular moment. (tr 93)

6. In a written program, the use of a variable in another function is called a "token" (tr 70). A token could mean almost anything, and when a program is running, the token substitutes a variable for another (tr 154). A token could be a user's unique identification.

7. DC 1. Illegal or unauthorized entry into any information technology system. E2.A13.1.2.1.