DATE: April 10, 1997

In Re:

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

Applicant for Security Clearance

ISCR OSD Case No. 96-0687

DECISION OF ADMINISTRATIVE JUDGE

JOHN R. ERCK

APPEARANCES

FOR THE GOVERNMENT

Pamela Benson, Esquire

Attorney Advisor

Barry M. Sax, Esquire

Department Counsel

FOR THE APPLICANT

Pro Se

STATEMENT OF THE CASE

On December 2, 1996, the Defense Office of Hearings and Appeals (DOHA), pursuant to Executive Order 10865, "*Safeguarding Classified Information Within Industry*," dated February 20, 1960, as amended and modified, and Department of Defense Directive 5220.6 *"Defense Industrial Personnel Security Clearance Review Program*" (Directive) dated January 2, 1992, as amended by Change 3, dated February 13, 1996, issued a Statement of Reasons (SOR) to Applicant which detailed reasons why DOHA could not make a preliminary determination that it was clearly consistent with the national interest to grant or continue a security clearance for him.

A copy of the SOR is attached to this Decision and included herein by reference.

The Applicant responded to the SOR on December 5, 1996 and requested a hearing before a DOHA Administrative Judge. The case was reassigned to this Administrative Judge on January 15, 1996 after having been previously assigned to another Administrative Judge on December 20, 1996. On February 4, 1997, a hearing was convened for the purpose of considering whether it would be clearly consistent with the national security to grant Applicant's security clearance. The Government's case consisted of five exhibits; Applicant relied on his own testimony. A transcript of the proceedings was received on February 12, 1996.

FINDINGS OF FACT

Applicant has admitted without explanation the factual allegations pertaining to personal conduct under Criterion E, the factual allegations pertaining to criminal conduct under Criterion J., and the factual allegations pertaining to misuse of information technology systems under Criterion M. After a complete and thorough review of the evidence in the record, and upon due consideration of the same, I make the following additional findings of fact:

Applicant is a 23 year old employee of a defense contractor with a Bachelor's Degree in computer science. He has worked for his current employer since April 1995 and is currently applying for a secret clearance. A favorable preliminary determination could not be made in his case because of evidence that he had been involved in criminal misconduct and in the misuse of information technology systems, and because he had then not been truthful in disclosing this information to the Department of Defense (DoD) during the background investigation conducted by the Defense Investigative Service (DIS).

While Applicant was attending college (from 1990 to 1994), he worked in the academic computer center (ACC) of the university (where he was enrolled) from June 1991 to June 1993. The ACC provided computers and many different, copyrighted software programs for student and faculty use. Applicant has admitted that he copied three of the center's software programs unto to disks for personal use on his own computer during the time he was employed by the ACC. He has admitted that his actions were both illegal and unethical (Gov. Exh 2). During the same time frame, Applicant accepted a software program which a friend of his had copied at the ACC. He knew that accepting copied software was a violation of copyright laws. Applicant has explained that he copied the software so that he could complete work at home that had been assigned to him by the ACC. Because of his knowledge of computers, he was consistently "bothered" by people seeking advice (Tr. 62). It became impossible for him to finish his work at ACC.

Later during his college career (from June 1993 to May 1994), Applicant worked at the university's technology transfer center (TTC). Again, he made copies of copyrighted computer software programs for use on his own computer. And again, Applicant used most of the copied software to complete work on assignments for his employer. However, he also made copies for friends on one or more occasions (Gov. Exh. 2). The software which Applicant copied for himself without authorization was also available for sale from his employer at a substantial discount (Tr. 60).

Although Applicant never asked permission to copy ACC or TTC's software, he believed that both employers knew that copies were being made (Tr. 73). He has rationalized that his actions were permitted--with respect to some of the software--by "something known as a shared license." Under this arrangement, copyrighted software could be re-copied on a home computer as long as it was used "eighty percent of the time" on the second computer for completion of the principal licensee's work. However, Applicant admitted that he had never asked his employers' permission with respect to any of the programs he had copied. (Tr. 73)

From 1992 to 1994, Applicant worked part-time for a company that sold tickets to ------- events. While employed in that capacity, he participated in an unauthorized and illegal scheme to the detriment of his employer. He sold large blocks of tickets to scalpers--against his employer's rules-- and accepted substantial tips from the scalper in return for the favor. Applicant also participated in a scheme whereby he would print tickets and then void them on the computer. He would then sell the printed tickets to scalpers or give them to friends. Applicant's participation in these schemes was not limited to one or two occasions, but was a regular occurrence during his tenure with this employer. He estimates that he earned $500.00 in kickbacks from scalpers, and that he eventually stole between 300 and 400 tickets from this employer in the two years that he worked for the company.

When asked to explain why he had stolen the tickets, Applicant identified "greed" as the principal motivation (Tr. 45). He had become frustrated because he not received a pay increase from this employer in the time he worked for him (Tr. 46). Earlier, in his first statement to the DIS (Gov. Exh 3), Applicant admitted that he knew stealing the tickets was wrong, but did it anyway. In the same statement, he explained to the DIS "that what some people might regard as unexplained affluence" was attributable to the fact that he had grown up in "a family of substantial means," and had had grandparents who had been "very generous."

As a result of his illegal activities, Applicant was arrested for larceny of tickets in July 1994. The charges against him were dropped after Applicant admitted that he had taken some tickets for his own use and agreed to reimburse his former employer $3,000.00. Applicant now admits that the value of the tickets stolen during the time of his employment

was far in excess of that amount (Tr. 48-49)

When he was first interviewed by the DIS on June 24, 1996, Applicant stated specifically that he had not copied any copyrighted computer software programs during the time that he was employed by ACC (Gov. Exh. 3). He acknowledged that he had been arrested in July 1994 and charged with grand larceny--a felony. However, he admitted that he had taken only 50 to 100 tickets from his former employer. He did not admit that the actual number of tickets he had stolen from his former employer was between 300 and 400 until the second DIS interview.

On his own behalf, Applicant testified that his involvement in the incidents alleged in the SOR was attributable to immaturity. He has learned from his mistakes and has become a better person. He is now married and has a wife and child about whom to be concerned.

POLICIES

The Adjudicative Guidelines of 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 with reasonable consistency that are clearly consistent with the interests of national security. In making those 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 the factors set forth in section F.3. 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 that the facts proven have a nexus to an applicant's lack of security worthiness.

The following Adjudicative Guidelines are deemed applicable to the instant matter.

PERSONAL CONDUCT

(Criterion E)

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

(3) Deliberately providing false or misleading information concerning relevant and material matters to an investigator,....or other official representative in connection with a personnel security or trustworthiness determination.

(5) A pattern of dishonesty or rule violations.

Conditions that could mitigate security concerns:

None applicable.

CRIMINAL CONDUCT

(Criterion J)

Conditions that raise a security concern and may be disqualifying:

(2) A single serious crime or multiple lesser offenses.

Conditions that could mitigate security concerns:

None Applicable

MISUSE OF INFORMATION TECHNOLOGY SYSTEMS

(Criterion M)

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.

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

(3) Removal (or use) of hardware, software or media from any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations.

Conditions that could mitigate security concerns include:

None Applicable

Burden of Proof

The Government has the burden of proving any controverted facts alleged in the Statement of Reasons. If the Government establishes its case, the burden of persuasion shifts to the applicant to establish his security suitability through evidence which refutes, mitigates, or extenuates the disqualifying conduct and demonstrates that 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 that Court's rationale, doubts are to be resolved against an applicant.

CONCLUSIONS

Having considered the record evidence in accordance with the appropriate legal precepts and factors, this Administrative Judge concludes that the Government has established its case with regard to Criteria E, J and M.

In reaching my decision, I have considered the evidence as a whole, including each of the factors enumerated in Section F.3, as well as those referred to in the section dealing with the Adjudicative Process, both in the Directive.

There is a common thread which runs through the allegations in the SOR. Applicant engaged in illegal activity after becoming frustrated in a work environment. At ACC and NTT, he copied computer software without asking permission because he wanted to work at home rather than at his employer's facility where he was being "bothered.". When he became frustrated with his work at the ticket sales company because he had not received a pay increase, he stole tickets to quiet his frustration.

Applicant's illegal actions are particularly bothersome because in each instance, he ignored obvious legal alternatives to engaging in activities which in addition to violating the law, also violated the trust of an employee--employer relationship. He could have asked his employers for permission to copy the software which would have enabled him to work at home. He could have purchased the software at a deep discount instead of resorting to an illegal and unethical means of self help. Applicant copied the software because it was easier than asking his employer's permission, and cheaper than purchasing the software. When he became frustrated in his work for the ticket company, he could have quit. He has indicated that he did not need this job to provide the necessities of life (Tr. 68). His family has "substantial means" and his grandparents have been "very generous." Applicant stole because he was greedy, not because he did not have a viable alternative.

Applicant then compounded his mistakes by not being honest and forthright about his activities when he was interviewed by the DIS, and when he signed the sworn statement on June 24, 1996.

Criterion E applies to "the deliberate omission...of relevant and material facts from any personnel security questionnaire...or deliberately providing false and misleading information...to an investigator in connection with a personnel security...determination." Facts are considered relevant and material when they are capable of influencing a federal agency's decision, e.g., a decision to grant or deny a security clearance. In this instance, Applicant's unauthorized copying of at least three copyrighted computer software programs from a former employer falls well within the definition of materiality. When he was initially asked about this activity during the first DIS interview, Applicant specifically denied that he had copied any software programs from his employer (Gov. Exh. 3). During the same interview, Applicant did not tell the truth about the number of tickets he had stolen from his former employer. He indicated that the total number of tickets stolen was between 50 and 100, when he had actually stolen between 300 and 400 tickets. This information was also relevant, material, and capable of influencing the DoD's decision on whether to grant Applicant a security clearance.

While Applicant is credited with eventually telling DIS the truth about the software copying and the ticket theft, there is no evidence that he made a prompt, good-faith effort to correct the falsification before being confronted with the facts. Nor is the falsification on Applicant's first statement to the DIS mitigated by the explanation he provided at his administrative hearing. His testimony that he did not think the copying issue would come up during the DIS interview (Tr. 32) does not excuse lying about it when--contrary to those expectations--the issue did come up. He testified that he did not tell the truth about the number of tickets he had stolen during the first DIS interview because he was nervous about being arrested again (Tr. 43-44). While Applicant's concern is understandable, it does not justify his signing a statement which included information that he knew was not true. Criterion E is concluded for Applicant.

The Government has met its burden with respect to Criterion J. Applicant has admitted that he stole tickets from his former employer with a value of several thousand dollars. As a result of his theft he was arrested for grand larceny, a felony. The charges against Applicant were later dropped after he agreed to reimburse his former employer $3000.00.

Applicant has also admitted that he was not truthful to an agent of the DIS when he was first interviewed on June 24, 1996. On that occasion, Applicant lied when he stated that he had never copied copyrighted software from a former employer. He lied again when he stated that he had stolen only 50-60 tickets from his former employer. He eventually admitted that he had stolen between 300 and 400 tickets from this employer. Applicant's willfully withholding this information from the DoD on matters that were clearly relevant to his security clearance eligibility violates 18 U.S.C. §1001. The information withheld by Applicant had the potential to influence the course of his background investigation in areas of legitimate concern to the DoD.

As mitigation for stealing tickets from the ticket sales company, Applicant has explained that he experienced "a serious level of frustration" when he was required to work "80 and 90 hour weeks and there was no compensation for overtime." Had the ticket theft occurred on one, isolated occasion, Applicant's explanation would be understandable and his one-time theft could be attributed to youthful indiscretion. However, it happened several times. Applicant had allowed the frustration to build where he could justify committing a crime. Instead of quitting at that point, he continued to work in that environment and he continued to steal tickets from his employer. Applicant's explanation for not being truthful about illegally copying computer software has been discussed (see above). Criterion J is concluded against Applicant.

With respect to Criterion M, Applicant has admitted that he copied several (six or more) computer software programs from two former employers without asking their permission or otherwise receiving proper authorization. Applicant knew that these programs were protected by copyright, and he has known since the age of 16 or 17 that it was "wrong" to copy such programs under the circumstances (Tr. 28-29).

Applicant's efforts to explain his actions provide some insight into how and why he did what he did, but his explanations do not mitigate the security concerns raised by his improper activities. He testified that he did not understand the implications of copying software when he first began using computers ten to twelve years ago. He and his friends routinely exchanged and copied computer programs from each other (Tr. 27) because he did not realize it was improper or unethical, and his parents did not know enough about computers to correct him (Tr. 28). Notwithstanding this lack of guidance from his parents, Applicant still learned that copying software was wrong. He testified that by the age of 16 or 17, he knew it was "wrong" to copy copyrighted software programs (Tr. 28-29).

I have carefully considered the circumstances under which Applicant copied software programs from his employer. Favorable consideration has been given to Applicant's testimony that he copied these programs primarily so that he could complete his employers' work assignments on his home computer (Tr. 63). Favorable consideration has also been given to Applicant's testimony that he did not personally profit from any of the software which he had illegally copied from his employers. However, this favorable evidence must be weighed against Applicant's testimony that he had never asked his employer for permission to copy the software so that he could complete assignments on his home computer,[(1)] and against Applicant's testimony that he compounded his illegal activity by distributing copies of some of the illegally copied software to his friends (Tr. 73). He has acknowledged that his friends did not use this software to complete work which had been assigned to Applicant (Tr. 63). Criterion M is concluded against Applicant.

FORMAL FINDINGS

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

Paragraph 1 (Criterion E) AGAINST THE APPLICANT

Subparagraph 1.a. Against the Applicant

Subparagraph 1.b. Against the Applicant

Paragraph 2 (Criterion J) AGAINST THE APPLICANT

Subparagraph 2.a. Against the Applicant

Subparagraph 2.b. Against the Applicant

Paragraph 3 (Criterion M) AGAINST THE APPLICANT

Subparagraph 3.a. Against the Applicant

Subparagraph 3.b. Against the Applicant

Subparagraph 3.c. Against the Applicant

DECISION

In light of all the circumstances presented by the record in this case, it is not clearly consistent with the national interest to continue Applicant's security clearance.

John R. Erck

Administrative Judge

1. Certain software licensing agreements include a provision under which an employer may allow an employee to copy software on his own computer, as along as it is used by the employee to work on his employer's business.