DATE: July 1, 2003

In Re:

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

Applicant for Security Clearance

ISCR Case No. 02-16216

DECISION OF ADMINISTRATIVE JUDGE

MARTIN H. MOGUL

APPEARANCES

FOR GOVERNMENT

Juan J. Rivera, Department Counsel

FOR APPLICANT

Pro Se

SYNOPSIS

Applicant committed larceny by taking from his place of employment, the National Security Agency (NSA), a considerable amount of computer hardware for his personal use, valued by his employer at more than $3,800. These computer hard drives contained classified information. Applicant received two non-judicial punishments. The first was for Larceny/Theft of National Defense Information (Title18 USC 641) and Wrongfully Retaining National Defense Information (Title18 USC 793), and the second was for cheating on a test by stealing the answer key from an Army safe. In a signed, sworn 1998 Security Clearance Application (SCA.) Applicant knowingly failed to disclose that he received the two Article 15s. Clearance is denied.

STATEMENT OF THE CASE

On November 7, 2002, the Defense Office of Hearings and Appeals (DOHA), pursuant to Executive Order 10865 and Department of Defense Directive 5220.6 (Directive), dated January 2, 1992, issued a Statement of Reasons (SOR) to Applicant which detailed 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 Applicant and recommended referral to an Administrative Judge to determine whether clearance should be denied or revoked.

In a signed and sworn statement, dated December 16, 2002, Applicant responded in writing to the SOR allegations. He requested a clearance decision based on a hearing record.

On February 4, 2003, this case was assigned to another Administrative Judge, but on February 10, 2003, because of caseload consideration, the case was reassigned to me to conduct a hearing and issue a written decision. A Notice of Hearing was issued to the parties on February 11, 2003, and the hearing was held on February 26, 2003.

At the hearing, Department Counsel offered 11 documentary exhibits (Government Exhibits 1 - 10) and no witnesses were called. Applicant offered 2 documentary exhibits (Applicant Exhibits A and B) and offered his own testimony. The transcript (TR) was received on March 5, 2003.

FINDINGS OF FACT

After a complete and thorough review of the evidence in the record, including Applicant's Answer to the SOR, the documents and the live testimony, and upon due consideration of that evidence, I make the following Findings of Fact: Applicant is a 29 year old employee of a defense contractor who seeks access to classified information.

In the SOR, the Government alleges that a security risk may exist under Adjudicative Guideline E (Personal Conduct), Guideline K (Security Violations) and Guideline J (Criminal Conduct) of the Directive. The SOR contains five allegations, 1.a. through 1.e., under Guideline E, two allegations 2.a. and 2.b. under Guideline K and two allegations 3.a. and 3.b. under Guideline J. In his signed, sworn response to the SOR, Applicant admits all of the allegations. Accordingly I incorporate those admissions as findings of fact. Additionally, I find as follows:

Applicant committed larceny by taking from his place of employment, the National Security Agency (NSA), a considerable amount of computer hardware for his personal use, valued by his employer at more than $3,800. The stolen equipment was found in Applicant's quarters during an investigation.(Exhibit 2.) Applicant believed that some of this hardware, in the form of hard drives, potentially contained classified documents. Applicant attempted to wipe out all of the classified information that was on these hard drives, but he was not successful in this attempt. (TR at 39.) It was determined that these computer hard drives, stolen by Applicant, contained classified information. (Exhibit 2.)

Initially, when Applicant was confronted by NSA agents about his unlawful conduct, Applicant denied, in a sworn statement that he signed on February 13, 1997, that he had illegally taken the computer parts. (Exhibit 4.) When he was subsequently confronted, he admitted that he had knowingly and illegally taken computer parts without authorization. He further admitted that he had lied about taking the computer parts because he, "was scared and didn't want to get in trouble." (Exhibit 5.)

On June 23, 1997, Applicant received a non-judicial punishment, an Article 15 under the United Code of Military Justice (UCMJ), for Larceny/Theft of National Defense Information (Title18 USC 641) and Wrongfully Retaining National Defense Information (Title18 USC 793). He was reduced in rank from an E4 to an E3 and given extra duty for 30 days. (Exhibit 9.)

On October 17, 1997, Applicant received a second non-judicial punishment, an Article 15, UCMJ, for cheating on a test by stealing the answer key from an Army safe, which is a violation of Article 107. He received an oral Reprimand and 10 days extra duty. (Exhibit 10)

In answering **Question 25** on his May 28, 1998 SCA, the Applicant failed to disclose the two Article 15s that he received; the one on June 23, 1997, for Larceny/Theft of National Defense Information (Title18 USC 641) and Wrongfully Retaining National Defense Information (Title18 USC 793) and the second one on October 17, 1997, for cheating on a test by stealing the answer key from an Army safe, as discussed above. Applicant knew that by not listing these Article 15s he was not being truthful with the information that he furnished to the Government, but he lied because he believed that he would not get a security clearance if he was honest. (Tr at 61.)

POLICIES

Enclosure 2 of the Directive sets forth adjudicative guidelines that must be carefully considered in evaluating an individual's security eligibility and making the overall common sense determination required. The Administrative Judge must take into account the conditions raising or mitigating security concerns in each area applicable to the facts and circumstances presented. 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, as the guidelines reflect consideration of those factors of seriousness, recency, motivation, *etc*.

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.

Each adjudicative decision must also include an assessment of: (1) the nature, extent, and seriousness of the conduct; (2)

the circumstances surrounding the conduct, and the extent of knowledgeable participation; (3) how recent and frequent the behavior was; (4) the individual's age and maturity at the time of the conduct; (5) the voluntariness of participation; (6) the presence or absence of rehabilitation and other pertinent 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 (See Directive, Section E2.2.1. of Enclosure 2).

Based upon a consideration of the evidence as a whole, I find the following adjudicative guidelines most pertinent to an evaluation of the facts of this case:

PERSONAL CONDUCT (GUIDELINE E)

E2A5.1.1. 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. . .

E2. A5.1.2. Conditions that could raise a security concern and may be disqualifying include:

E2.A5.1.2.2. 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, . . . [or] determine security clearance eligibility or trustworthiness. . .;

E2.A5.1.2.3. Deliberately providing false or misleading information concerning relevant and material matters to an investigator, security official . . . in connection with a personnel security or trustworthiness determination;

E2.A5.1.2.5 A pattern of dishonesty or rules violations of any written or recorded agreement made between the individual and the agency;

E2.A5.1.3. Conditions that could mitigate security concerns include:

None.

SECURITY VIOLATIONS (GUIDELINE K)

E2.A11.1.1. The Concern: Noncompliance with security regulations raises doubt about an individual's trustworthiness, willingness, and ability to safeguard classified information.

E2.A11.1.2. Conditions that could raise a security concern and may be disqualifying include:

E2.A11.1.2. 2. Violations that are deliberate or multiple or due to negligence.

E2.A11.1.3. Conditions that could mitigate security concerns include actions that:

None

CRIMINAL CONDUCT (GUIDELINE J)

E2.A10.1.1. The Concern: A history or pattern of criminal activity creates doubt about a person's judgment, reliability and trustworthiness.

E2.A10.1.2. Conditions that could raise a security concern and may be disqualifying include:

E2.A10.1.2.1. Allegations or admissions of criminal conduct, regardless of whether the person was formally charged;

E2.A10.1.2.2. A single serious crime or multiple lesser offenses.

E2.A10.1.3. Conditions that could mitigate security concerns include:

None.

BURDEN OF PROOF

Initially, the Government must prove controverted facts alleged in the Statement of Reasons. If the Government meets that burden, the burden of persuasion then shifts to Applicant to establish his security suitability through evidence of refutation, extenuation or mitigation sufficient to demonstrate that, despite the existence of disqualifying conduct, it is nevertheless clearly consistent with the national interest to grant or continue the security clearance. Assessment of Applicant's fitness for access to classified information requires evaluation of the whole person, and consideration of such factors as the recency and frequency of the disqualifying conduct, the likelihood of recurrence, and evidence of rehabilitation.

A person who seeks access to classified information enters into a fiduciary relationship with the U.S. Government that is predicated upon trust and confidence. Where facts proven by the Government raise doubts about Applicant's judgment, reliability, or trustworthiness, Applicant has a heavy burden of persuasion to demonstrate that he or she is nonetheless security worthy. As noted by the United States Supreme Court in Department of the 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."

CONCLUSIONS

Having considered the evidence of record in light of the appropriate legal precepts and factors, I conclude the following with respect to guidelines E, K and J:

With respect to Guideline E, the evidence establishes that Applicant intentionally provided false material information to the Government in response to a question on the SCA that he executed in May 1998. The Government relies heavily on the honesty and integrity of individuals seeking access to our nation's secrets. When such an individual intentionally falsifies material facts on a security clearance application, it is extremely difficult to conclude that he nevertheless possesses the judgment, and honesty necessary for an individual given a clearance . In this case, Applicant's falsifications of his SCA was knowingly and willingly committed in an attempt to obtain employment and a security clearance.

Additionally, under Guideline E, Applicant's conduct regarding the knowing and willful theft of Government computers, which resulted in his receiving an Article 15, and his stealing an answer key for a test, which resulted in his receiving a second Article 15, also shows conduct of an individual who does not have the requisite reliability and trustworthiness required of clearance holders. I resolve Guideline E against Applicant.

In reviewing the Disqualifying Conditions (DC) under Guideline E, I conclude that DC 2 and DC 3 apply because of the false information that Applicant provided in his SCA and to NSA investigators. DC 5 also applies because of Applicant's dishonesty in stealing Government computers. No Mitigating Conditions (MC) apply.

Guideline K has been established by the Government. Applicant's theft of NSA computers that contained classified information is a deliberate violation of security procedures. I resolve Guideline K against the Applicant.

I conclude DC 2 applies because Applicant's act was a deliberate violation of security procedures. No MCs apply.

Finally, the Government has established its case under Guideline J. Applicant's theft of NSA computer parts including hard drives containing classified information is criminal conduct that violates 18 U.S.C. §641 and §793. I resolve Guideline J against the Applicant.

Under Guideline J, I conclude that DC 2 applies because Applicant theft of NSA computers is an extremely serious crime. No MCs apply.

FORMAL FINDINGS

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

Paragraph 1. Guideline E: AGAINST THE APPLICANT

Subparagraph 1. a.: Against the Applicant

Subparagraph 1.b.: Against the Applicant

Subparagraph 1.c.: Against the Applicant

Subparagraph 1.d.: Against the Applicant

Subparagraph 1.e.: Against the Applicant

Paragraph 2. Guideline K: AGAINST THE APPLICANT

Subparagraph 2.a.: Against the Applicant

Subparagraph 2.b.: Against or the Applicant

Paragraph 3. Guideline J: AGAINST THE APPLICANT

Subparagraph 1. a.: 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 grant or continue a security clearance for Applicant.

_____

Martin H. Mogul

Administrative Judge