DATE: November 16, 2004

In Re:

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

Applicant for Security Clearance

ISCR Case No. 02-32290

ECISION OF ADMINISTRATIVE JUDGE

DARLENE LOKEY ANDERSON

APPEARANCES

FOR GOVERNMENT

Edward W. Loughran, Department Counsel

FOR APPLICANT

Thomas W. Abbott, Attorney At Law

SYNOPSIS

The Applicant committed three security violations, one in 1985, one in 1988 and one in1998. He has not committed a security violation in the last six years. His security violations have been mitigated by a sufficient showing of reform and rehabilitation. Clearance is granted.

STATEMENT OF THE CASE

On December 31, 2003, 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 January 26, 2004 and requested a hearing before a DOHA Administrative Judge. This case was assigned to the undersigned on April 8, 2004. A notice of hearing was issued on April 27, 2004, scheduling the hearing for June 15, 2004. Applicant's counsel requested a continuance on June 8, 2004. The matter was continued until August 4, 2004. At the hearing the Government presented six exhibits. The Applicant presented eight exhibits and he testified on his own behalf. The official transcript (Tr.) was received on August 23, 2004.

FINDINGS OF FACT

The following Findings of Fact are based on Applicant's Answer to the SOR, his testimony and the documents. The Applicant is 59 years of age, has an Engineering fellowship and is employed by a defense contractor. He seeks a security clearance in connection with his employment in the defense industry.

Paragraph 1 (Guideline K- Security Violations). The Government alleges that the Applicant's noncompliance with security regulations may raise doubts about his trustworthiness, willingness, and ability to safeguard classified information.

Paragraph 2 (Guideline M - Misuse of Information Technology Systems). The Government alleges that the Applicant's noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about his trustworthiness, willingness, and ability to properly protect classified systems, networks, and information.

Paragraph 3 (Guideline E - Personal Conduct). The Government alleges that the Applicant is ineligible for clearance because he has engaged in conduct involving questionable judgment, untrustworthiness, unreliability, or unwillingness to comply with rules and regulations.

The Applicant has been employed in the defense industry for thirty years. He received his first security clearance in the early 70's.

In 1985, the Applicant left his safe that contained classified materials unlocked. The Applicant contends that he spun the dial to lock his safe, but obviously did not spin it enough. A security guard while demonstrating to someone else how to check the safe, spun the lock, turned the latch, and the Applicant's safe opened. This surprised both the Applicant and the security guard. A security violation was issued to the Applicant. This was a violation of company rules, procedures and guidelines and a violation of paragraph 14 of DoD 5220.22-M, the Industrial Security Manual(ISM), dated December 1985. The Applicant received a written reprimand for this violation. The Applicant testified that since then he has learned to properly spin the lock. He then goes around and checks the other safes in the area by spinning them in the forward direction

In February 1989, the Applicant was working on a proposal using classified materials. During a conference call he disclosed Secret classified information to an uncleared personnel by providing a Secret document to a secretary to fax an unclassified portion of the document without authorization. Providing a classified document to an uncleared individual is a security violation. This was a violation of company rules, procedure and guidelines and a violation of paragraph 17 of DoD 5220.22-M, the Industrial Security Manual (ISM), dated November 1986. The Applicant explained that he was preoccupied when he handed the classified document to the uncleared secretary. It did not occur to him that the document was classified or that he should check to see if the person was wearing a badge indicating that they were cleared or not before giving the classified document to them. (Tr. P. 25). The Applicant testified that the uncleared secretary was new to his department and had recently been assigned him. She did not work in his department long. The Applicant received a security violation for this conduct. The Applicant was subsequently advised of his responsibility to protect classified information in his possession.

In May 1998, while working in a secured environment, (a SCIF) the Applicant knowingly removed a file from a classified computer system without authorization. Since the file or disk was used on a classified computer, the disk became classified. It was also discovered through a search of the Applicant's computer and his files that he had classified materials at the confidential level on his home computer. The Applicant admitted that he downloaded information form his computer hard drive at work and transferred it to a floppy disk. He then brought the disk home. He downloaded the information on the floppy disk to his home computer hard drive. By doing this, he improperly removed, stored and transported the classified information without authorization to do so. This was a violation of company rules, procedure and guidelines and a violation of paragraphs 5-100, 5-304, 5-404 and 8-100 of DoD 5220.22-M, the National Industrial Security Program Operating Manual (NISPOM), dated January 1995. The Applicant further explained that if he were to have followed proper company procedures, he would have taken the floppy disk to the company Security Office and told them that he believed the disk to be unclassified and that he would like to remove it. Instead, because the security department was slow at getting to this task, the Applicant took the disk, realizing at the time that he was committing a security violation. The Applicant received a security violation for this conduct and was suspended for a week without pay. (Tr. p. 22).

The Applicant explained that he has no excuse for his three security violations. He realizes the seriousness of his misconduct and does not expect them to ever happen again. He states that he is always very careful now when working

with or handling classified information.

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:

Security Violations

Noncompliance with security regulations raises doubt about an individual's trustworthiness, willingness, and ability to safeguard classified information.

Conditions that could raise a security concern:

1. Unauthorized disclosure of classified information;

2. Violations that are deliberate or multiple or due to negligence.

Conditions that could mitigate security concerns:

1. Were inadvertent;

2. Were isolated and infrequent;

4. Demonstrates a positive attitude towards the discharge of security responsibilities.

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:

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

3. Introduction of hardware, software or media into any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations.

Conditions that could mitigate security concerns:

1. The misuse was not recent or significant;

2. The conduct was unintentional or inadvertent;

3. The misuse was an isolated event.

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:

4. Personal conduct or concealment of information that increases an individual's vulnerability to coercion, exploitation or pressure;

5. A pattern of dishonesty or rule violations; to include violation of any written or recorded agreement made between the individual and the agency.

Condition that could mitigate security concerns:

5. The individual has taken positive steps to significantly reduce or eliminate vulnerability to coercion, exploitation, or duress.

In addition, as set forth in Enclosure 2 of the Directive at page 2-1, "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 an acceptable security risk. 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. All 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 K, (Security Violations), Guideline M (Misuse of Information Technology Systems), and Guideline E (Personal Conduct) which 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 a disregard for security policies and procedure, or who engages in a pattern of rule violations, may be prone to provide information or make decisions that are harmful to the interests of the United States. 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 of record in light of the appropriate legal standards and factors, and having assessed the Applicant's credibility, this Administrative Judge concludes that the Government has established its case as to all allegations in the SOR, and that Applicant's security violations, misuse of information technology systems and his personal conduct have a direct and negative impact on his suitability for access to classified information.

Considering all of the evidence, the Applicant has introduced persuasive evidence in rebuttal, explanation or mitigation that is sufficient to overcome the Government's case.

During the approximate thirty year period the Applicant was employed with the defense industry, he has committed three security violations prohibited by his company rules, procedure, and guidelines. He has also violated specific provisions of the Industrial Security Manual in affect at the time of the violations. None of the security violations were committed with deliberate or reckless disregard for company policy or defense industry procedures. Each violation is different and was committed inadvertently. Each violation occurred several years apart. In each instance, the Applicant learned that he must be more careful in handling classified information. The Applicant has not committed any security violation in six years. He has taken these violations seriously and realizes that he cannot commit any more. Under Guideline K, mitigating conditions, 1. *The violations were inadvertent*, 2. *The violations were isolated and infrequent*, and 4. *The Applicant demonstrates a positive attitude towards the discharge of security responsibilities* apply. Under Guideline M, mitigating conditions 1. *The misuse was not recent or significant* 2. *The conduct was unintentional or inadvertent,* 3. *The misuse was an isolated event* apply. Under Guideline E, mitigating condition 5. *The individual has taken positive steps to significantly reduce or eliminate vulnerability to coercion, exploitation, or duress* applies.

This Applicant has demonstrated that he is trustworthy, and does meet the eligibility requirements for access to classified information. Accordingly, I find for the Applicant under Guideline K (Security Violations), Guideline M (Misuse of Information Technology Systems), and Guideline E (Personal Conduct).

Considering all the evidence, the Applicant has rebutted the Government's case regarding his security violations, misuse of computer technology and personal conduct. The Applicant has met the mitigating conditions of Guidelines K, M or E of Section F.3. of the Directive. Accordingly, he has met his ultimate burden of persuasion under Guidelines K, M 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: For the Applicant.

Subparas. 1.a.: For the Applicant

1.b.: For the Applicant

1.c.: For the Applicant

1.d.: For the Applicant

1.e.: For the Applicant

1.f.: For the Applicant

Paragraph 2: For the Applicant.

Subparas. 2.a.: For the Applicant

Paragraph 3: For the Applicant.

Subparas. 3.a.: For the Applicant

DECISION

In light of the circumstances presented by the record in this case, it is clearly consistent with the interests of national security to grant or continue a security clearance for the Applicant.

Darlene Lokey Anderson

Administrative Judge