DATE: August 23, 2006

In Re:

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

Applicant for Security Clearance

ISCR Case No. 03-23829

ECISION OF ADMINISTRATIVE JUDGE

DARLENE LOKEY ANDERSON

APPEARANCES

FOR GOVERNMENT

Rita C. O'Brien, Department Counsel

FOR APPLICANT

Pro Se

SYNOPSIS

The Applicant's pattern of security violations, improper use of a government company computer, and personal conduct are in violation of company policies and procedures and have not been mitigated. Clearance is denied.

STATEMENT OF THE CASE

On August 2, 2005, 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 August 26, 2005, in which he elected to have the case determined on a written record in lieu of a hearing. Applicant's company notified DOHA on October 25, 2005, that because of hurricanes in his local area, the Applicant has lost his original SOR and attached documents DOHA forwarded to him in August. A second set was forwarded to him on October 26, 2005, through his Facility Security Officer. The Applicant signed for the second set of documents on October 31, 2005. Department Counsel submitted the Government's File of Relevant Material (FORM) to the Applicant on February 15, 2006. The Applicant was instructed to submit information in rebuttal, extenuation or mitigation within 30 days of receipt. Applicant received the FORM on February 22, 2006, and he submitted a response dated March 21, 2006, and a second response dated May 15, 2006. Department Counsel objected to Applicant's response dated March 21, 2006. The Government's objection was overruled and both of Applicant's responses were admitted into evidence. The case was assigned to the undersigned for resolution on April 27, 2006.

FINDINGS OF FACT

The following Findings of Fact are based on Applicant's Answer to the SOR, and the documents. The Applicant is 58 years of age, and holds a Bachelor's and a Master's Degree of Science in Physics. He is employed as a Senior Scientist 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 raises doubt about an individual's 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.

The Applicant was granted a Secret level security clearance in 1967. This clearance was upgraded to Top Secret in about 1985, and then upgraded again to SCI access in about 1988. He maintained Special Access clearances to attend various technical and intelligence meets and to conduct analysis on technical projects. All of his clearances were suspended during an Naval Criminal Investigative Service (NCIS) investigation beginning in August 2002.

In 1986 or 1987, the Applicant admits that he knowingly failed to follow proper procedure when he allowed his secretary, who was cleared only to the secret level and not did have a NATO security clearance to hand carry a classified NATO document to an adjacent building. The Applicant explained that although he had, at the time, held a secret clearance for almost twenty years, he had only had NATO access for about a year and was not aware of its sensitivity. Following this incident, the Applicant became aware of the importance of NATO access and has not had any problems since then with the handling of NATO materials. (*See* Government Exhibit 4).

The Government alleges that from approximately April 2002 to August 2002, the Applicant transmitted classified information via unclassified e-mail which is against security policies. When the error was discovered, he instructed his team in how to sanitize the computer system rather than bring the error to the attention of his security officer or supervisor. The Applicant adamantly denies this allegation. (*See* Government Exhibit 4, 6 and 7). There is evidence that in 2002, the Applicant led a team on a certain program at a Research Laboratory (RL). As a part of a field exercise, the Applicant and his team members, were each deployed to a different state. During their deployment, they exchanged e-mails concerning the program on the unclassified RL network.

In August 2002, one team member reported to the Department Head that he had security concerns about the events during and following the program exercise. According to the Department Head's Memorandum for the Record, the program data was not as accurate as the Applicant had thought and that he should breakdown the files to a readable form. Two of the Applicant's team members tried to convince the Applicant not to do this as it would pose a security risk, but the Applicant insisted. This resulted in a definite compromise of confidential data. (*See* Government Exhibits 7 and 8).

A security background memorandum dated August 19, 2002, states that, "When finally convinced that a compromise could have occurred, [the Applicant] directed the removal of the offending data files from all computer systems on which they were resident. [The Applicant] did not report any of this to his branch or the security office." (*See* Government Exhibit 8).

The Applicant's version of the events is different. He stated that as soon as he learned of the error, he instructed his team members to make the correction. The Applicant asserts that once he discovered the security compromises, he made the changes necessary to protect the classified information. He states that one of the his team members argued strongly against deleting the data but the Applicant insisted that it be done. This interchange involved roughly two dozen e-mails and occurred over about a 2 or 3 day period. (*See* Government Exhibits 4 and 6).

Given the restrictions of this forum, I have reviewed all of the available evidence including the (NCIS) investigation concerning this matter. Based upon my analysis of the available evidence, the evidence is mixed and confusing and it is impossible to determine where the truth lies. Under the circumstances, I cannot find that the Applicant was negligent or that he failed to follow policy security policies and procedures. Accordingly, subparagraph 1(b), is found for the

Applicant. (*See* Government Exhibit 4).

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.

Prior to 2002, the Applicant purchased a laptop computer with government funds. The Applicant allowed his son, who is not a government employee, to use the laptop. The Applicant explained that he purchased the laptop because it was lightweight and would be easy for him to use as carry-on baggage on business trips. The Applicant states that he asked his son to set up the computer because of his computer expertise. The Applicant states that both he and his son used the laptop. (*See* Government Exhibit 4). This claim, however, contradicts Applicant's repeated statement at the time of the event when he informed his Security Manager that only his son used the computer at their residence. (*See* Government Exhibit 9).

On July 5, 2002, the Applicant knowingly allowed his twenty year old son unescorted access to a (RL) workspace. The Applicant's son was signed in at the gate, as an "escort required", visitor. His son was not escorted as other employees saw him alone. The Applicant's son sat in the office immediately adjacent to the Applicant's. The Applicant was not authorized to do this and this action was in blatant disregard of company policies concerning computer security and usage procedures. (*See* Government Exhibit 9).

On July 5, 2002, the Applicant also knowingly allowed his son to have unsupervised access to a government network. The Applicant explained that he knew that his son would be searching for and downloading software onto the lightweight government computer. The Applicant did not supervise his son during this process and his son hacked into the RL server, and downloaded pornographic material by using the identity of another government employee by using the persons Internet Protocol address. The Applicant's son had told him that just entering an IP address on the computer would allow access to the network. The company policy clearly prohibits a non-government employee to be attached to the government network. (*See* Government Exhibit 9).

The Applicant claims that the pornographic material downloaded by his son on the government computer by using the identity of another government employee was "adult" pornography. (*See* Government Exhibit 6). The Security Officer's Report dated July 10, 2002 notes that the Navy's investigation revealed that the "hostile appears to be downloading child pornography." (*See* Government Exhibit 9).

The company security department took action against the Applicant for these security violations. The Applicant's dial-in account was de-activated. His key card access has been limited to normal working hours, and his son has been barred from site access. (*See* Government Exhibit 9).

Four letters of recommendation from people who know the Applicant well, including his most recent former supervisor at RL, another former supervisor, his current supervisor and Vice President of the company, and a Government Program Manager, all attest to his good character, reliability, trustworthiness, technical credentials, attention to detail, dedication to the job, and value to the national security. (*See* Applicant's Response to FORM).

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.

1. Unauthorized disclosure of classified information;

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

Conditions that could mitigate security concerns included actions that:

None.

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.

Condition that could mitigate security concerns:

None.

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:

None.

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 not introduced persuasive evidence in rebuttal, explanation or mitigation that is sufficient to overcome the Government's case.

There is no reasonable or acceptable excuse for the Applicant's history of repeated security violations and his misuse of information technology systems. His actions were deliberate and with blatant disregard for the rules and regulations for the proper safeguarding of classified information. The safety of such information is the ultimate goal of national security. The Government cannot continue to place its trust in one who repeatedly violates that trust by circumventing

security regulations.

The Applicant knowingly failed to follow company security policy and procedure in 1987, by allowing his secretary who was cleared secret without a NATO clearance to hand carry a classified NATO document to another building. In 2002, he again repeatedly violated company policy and procedure by purchasing a laptop with government funds to be used by his son who is not a government employee (committing a possible fraud), by knowingly allowing his son unescorted access to the company's workspace, and by knowingly allowing his son to have unsupervised access to a government network, where he used the identity of another government employee by using that person's Internet Protocols address and downloaded pornographic material. The most recent of these security violations occurred just four years ago. The Applicant's conduct establishes a pattern of rule violations and shows extremely poor judgment.

Under Guideline K, Disqualifying Conditions *(1) unauthorized disclosure of classified information* and *(2) violations that are deliberate or multiple or due to negligence* apply. None of the mitigating conditions are applicable. It was not inadvertent, unintentional, isolated or infrequent nor was it due to improper or inadequate training. Under Guideline M, Disqualifying Condition *(1) Illegal or unauthorized entry into any information technology system* applies. None of the mitigating conditions are applicable. Under Guideline E, Disqualifying Conditions *(4) Personal conduct or concealment of information that increases an individual's vulnerability to coercion, exploitation or pressure* and *(5) A pattern of dishonesty or rule violations; to include violation of any written or recorded agreement made between the individual and the agency* apply. None of the mitigating conditions are applicable.

This Applicant has not demonstrated that he is trustworthy, and does not meet the eligibility requirements for access to classified information at this time. He may be eligible some time in the future. Accordingly, I find against the Applicant under Guideline K (Security Violations), Guideline M (Misuse of Information Technology Systems), and Guideline E (Personal Conduct).

Furthermore, the Applicant has not provided this Administrative Judge with sufficient evidence in mitigation that would mitigate the negative impact his poor judgment has had on his security worthiness. At this time, I cannot find that it is clearly consistent with the national interests to grant the Applicant a security clearance.

Considering all the evidence, the Applicant has not rebutted the Government's case regarding his security violations, misuse of computer technology and personal conduct. The Applicant has not met the mitigating conditions of Guidelines K, M or E of Section F.3. of the Directive. Accordingly, he has not met his ultimate burden of persuasion under Guidelines K, M or 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.: For the Applicant

Paragraph 2: Against the Applicant.

Subparas. 2.a.: Against the Applicant

Paragraph 3: Against the Applicant.

Subparas. 3.a.: Against the Applicant

3.b.: Against the Applicant

3.c.: Against the Applicant

DECISION

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

Darlene Lokey Anderson

Administrative Judge