DATE: March 28, 2003

In Re:

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

Applicant for Security Clearance

ISCR Case No. 01-10012

DECISION OF ADMINISTRATIVE JUDGE

KATHRYN MOEN BRAEMAN

APPEARANCES

FOR GOVERNMENT

Erin C. Hogan, Esquire, Deputy Chief Department Counsel

FOR APPLICANT

Pro Se

SYNOPSIS

Applicant's security violations and personal conduct raise security concerns as in October 2000 he deliberately violated multiple security regulations and failed to meet his duty to inform his Facility Security Officer (FSO) that he had received a CD-Rom containing classified NATO information. While he justified his actions by a need to expedite a corporate bid proposal, he had been properly briefed on NATO security practices which he deliberately failed to follow even though he knew that such infractions were against his company's and the government's security requirements. While he otherwise has a fine employment record, such excellence on the job does not mitigate the security significance of his repeated and knowing deliberate security violations. Clearance is denied.

STATEMENT OF THE CASE

The Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) to the Applicant on July 19, 2002. The SOR detailed reasons why the Government could not make the preliminary positive finding that it is clearly consistent with the national interest to grant or continue a security clearance for Applicant.[(1)] The SOR alleges specific concerns over security violations (Guideline K) and personal conduct (Guideline E). Applicant responded to these SOR allegations in an Answer notarized on August 12, 2002, where he admitted allegation 1.a., 1.a.(1), (4), (5) and requested a hearing.

The case was assigned to Department Counsel who on October 10, 2002, attested it was ready to proceed; and the case was assigned to another administrative judge, John Erck. On October 16, 2002, the case was re-assigned to me. Subsequently, after a mutually convenient date for hearing was agreed to, a Notice of Hearing was issued on November 14, 2002, which set the matter for December 12, 2002, at a location near where Applicant works and lives. At the hearing the Government asked that I take official notice (ON) of two documents (ON I & II; TR 29-32) and offered into evidence fifteen Government exhibits; all were admitted into evidence. (Exhibits 1-15; TR 16-29, 45-46) The Government called one witness. The Applicant represented himself and offered one exhibit which was admitted into evidence. (Exhibit A) (TR 57-58) Applicant testified and called one witness. The transcript (TR) was received on

December 20, 2002.

FINDINGS OF FACT

After a complete and thorough review of the evidence in the record, and upon due consideration of that evidence, I make the following Findings of Fact:

Applicant, 53 years old, has worked for Defense Contractor #1 in State #1 since 1992. He was granted a Secret security clearance in September 1992 and in ay 1998. He served in the military from 1969 to 1992, when he retired as a major. (Exhibits 1, 2; TR 91-94) He no longer needs a security clearance to perform his current job. (TR 91-92, 124-125)

He has a BS degree in aviation management. (TR 91)

Security Violations and Personal Conduct

Applicant has had numerous contacts with foreign business people and with military and government personnel through business dealings at his corporation. He had a security clearance for 31 years without a security violation until the incident described below; this 2000 incident was the first time he possessed classified material that was not obtained within regulations and the first time he deceived a security official. (Exhibit 6, p. 4; TR 89-90)

When Applicant joined the corporation, he had an initial security briefing in August 1992 which included all corporate security procedures. His international security requirements briefings were frequent, verbal, but not documented. (Exhibit 9)

Applicant documented that he had received and read the corporate Security Practices Procedures (SPP) in August 1992. He declared that he understood that it was his responsibility to follow the instructions in the manual regarding security procedures; and if he did not understand a specific procedure or if he had a question regarding any security issue, he was to ask the Facility Security Officer (FSO) or the Deputy FSO for a resolution. (Exhibit 10) He signed a Classified Information Nondisclosure Agreement in August 1992. (Exhibit 12) He also received regular updated briefings. (Exhibit 13)

Applicant was briefed on his responsibilities for safeguarding NATO classified information in July 1996 and again in November 1997. Requirements for safeguarding United States classified information apply to NATO classified information. (Exhibit 11) Applicant believed he had adequate training. (TR 89)

While he was away from the office in September 2000, Applicant received through the US mail from a Greek marketing consultant an unmarked CD-ROM which consisted of operational and technical requirements for a procurement effort and which included NATO Confidential information. When he returned from a trip, Applicant stated that he saw no classification markings or transmittal information on the envelope and threw the envelope away. In initially viewing the CD, he saw no classification markings and locked it in his desk. In mid-October 2000 Applicant looked more closely at the CD and recognized it contained information on a NATO project for which the company wanted to submit a bid. He also noticed the NATO classified markings[(2)] - NATO Confidential (NATO-C) and NATO Restricted (NATO-R)[(3)] information. Applicant then made a "conscious business decision" not to inform the FSO of the improper[(4)] receipt of this classified information and to retain the information in his possession as he was under a tight time constraint to develop the proposal. He decided to use this classified information even though he later admitted he "knew it was wrong." As the proposal manager, Mr. O, also needed the information, Applicant printed a hard copy of portions of the CD on a printer connected to the LAN. He made a copy on the machine closest to his office and gave a copy of the information he had printed from the CD to Mr. O, a corporate international marking representative. Applicant instructed another employee make a copy[(5)] of the CD for Mr. O without advising her of its contents being classified NATO Confidential. Mr. O knew that there was NATO confidential information and agreed with Applicant not to report the improper receipt and safeguarding of the document to the FSO as they concluded it would be helpful to have access to the information while they waited for it to come through "proper channels." Applicant kept the CD and a hard copy locked in his desk when not in use which was not the proper storage required for NATO Confidential. (Exhibits 2, 6, 15; TR 36-39, 41-43, 44-45, 63-69, 73-75, 79-89) While his storing it in a locked file drawer was sufficient for NATO

Restricted information, Applicant admitted that was not proper storage for NATO Confidential under provision 10-710. (TR 77-79)

The FSO in November 2000 discovered this NATO Confidential material in the possession of Mr. O when she was assisting him in the proper transmission of a proposal by a foreign citizen. The information had also been shared with Mr. C. The FSO reported the violations to management, to DSS, and then initiated an investigation. Applicant stated to the FSO that he made two mistakes: "One is that I didn't remove ALL the NATO C markings" and two that he gave it to Mr. O. (Exhibits 2, 3, 4, 5; TR 69-72)

Applicant agreed that at the time he discovered the CD contained NATO classified information, he knew this was a security violation that should have been reported to the FSO. He did not report it because he was focused on preparing the proposal. Also, he explained he justified his conduct by other's practices as elsewhere the information was discussed "without it being treated as classified information."[(6)] (TR 75-76; 94-95)

This NATO Confidential information was placed on a Local Area Network (LAN) which resulted in "A LAN contamination[(7)] and on a personal computer located in an employee's home." Applicant and his colleague made a conscious business decision to retain the NATO Confidential Information without advising the FSO of its receipt and without implementing proper safeguarding[(8)] procedures. In November 2000 Applicant's corporation filed an Administrative Inquiry (AI) and a report required by the ***Industrial Security Operating Manual (ISOM)***, DSS 31-4M, with the Defense Security Service (DSS) that Applicant and a colleague had shown a "willful disregard for security regulations and requirements which did not result on the compromise of classified information"; Applicant showed a "clear pattern of negligent conduct in handling or storing classified information." (Exhibits 2, 3)

The SPP states that "Violations committed intentionally are subject to immediate termination of the employee's security clearance and/or dismissal from employment." (Exhibit 2) The corporation sent Applicant a letter that he had committed a serious violation and that any subsequent behavior would be cause for termination. (TR 92)

Clearance Suspended

On April 18, 2001, the Director of DSS took an interim action and advised Applicant that his Secret personnel security clearance granted to him was suspended based on his "willful disregard for security regulations and requirements" when he received a classified CD-ROM via regular mail from a Greek marketing representative, printed a hard copy of portions of the CD-ROM on a printer connection to his company's LAN and retained a copy of the CD-ROM and a hard copy of the information in a locked drawer in his desk. He also gave the classified CD-ROM to another employee and had her reproduce the CD-ROM, and he then provided the CD-ROM and a printed copy of the information to Mr. O. He admitted to deliberately not informing the FSO of his company of the existence and presence of the classified information. DSS provided a copy of the letter to his FSO. (Exhibit 14)

Applicant has not had any access to classified information since the security violation was discovered by the FSO in November 2000; he has removed himself from any aspect of classified information. (TR 89-90)

Reference

A corporate manager, Mr. A, who is now a vice-president testified that he initially met Applicant when he worked for the military in 1988 and was the program manager on a project where Mr. A was the corporate liaison for the program. At that time Applicant did not have a cavalier attitude toward classified information. After Applicant came to the corporation, Mr. A supervised Applicant for six years prior to this incident and is now again his supervisor. The manager assesses Applicant as "an exemplary employee" and a key resource. Mr. A recruited Applicant to work for him in 2001 and recently promoted Applicant to a new position to handle international programs and has entrusted a lot of responsibility to him as he has faith in Applicant. He believes Applicant made a mistake and has been punished for that mistake, but Applicant now works in an unclassified area of the corporation. Applicant has access to business sensitive information, but the manager has no concerns about Applicant handling it properly. Applicant has had all favorable evaluations. (TR 97-108)

POLICIES

Enclosure 2 of the Directive sets forth adjudicative guidelines to consider in evaluating an individual's security eligibility. They are divided into conditions that could raise a security concern and may be disqualifying and conditions that could mitigate security concerns in deciding whether to grant or continue an individual's access to classified information. But the mere presence or absence of any given adjudication policy condition is not decisive. Based on a consideration of the evidence as a whole, I weighed relevant Adjudication Guidelines as set forth below :

Guideline K - 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 and may be disqualifying include:

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

Conditions that could mitigate security concerns include actions that:

None

Guideline E - 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 and may be disqualifying also include:

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

Conditions that could mitigate security concerns include:

None

The responsibility for producing evidence initially falls on the Government to demonstrate that it is not clearly consistent with the national interest to grant or continue Applicant's access to classified information. The Applicant presents evidence to refute, explain, extenuate, or mitigate in order to overcome the doubts raised by the Government, and to demonstrate persuasively that it is clearly consistent with the national interest to grant or continue the clearance. Under the provisions of Executive Order 10865, as amended, and the Directive, a decision to grant or continue an applicant's security clearance may be made only after an affirmative finding that to do so is clearly consistent with the national interest. In reaching the fair and impartial overall common sense determination, the Administrative Judge may draw only those inferences and conclusions that have a reasonable and logical basis in the evidence of record.

CONCLUSIONS

Security Violations

The Government established security concerns over Applicant's five security violations in October to November 2000 based on his willfully disregarded security regulations and requirements when he (1) received a classified CD-ROM via regular mail from a Greek marketing representative, (2) had another employee copy the CD without advising it contained NATO classified information, (3) printed a hard copy of portions of the CD on a non-accredited AIS printer connected to his company's LAN, (4) improperly stored a copy of the CD and a hard copy of the information in a locked drawer in his desk, and (5) failed to physically mark CDs with the appropriate NATO Confidential classification markings. While in his answer Applicant denied he gave the classified CD to another employee and had her reproduce

the classified CD, the AI done by the corporation established this fact. Further, while he denied improperly printing the classified CD on a non-accredited AIS, the AI also established that fact. He then provided the CD and a printed copy of the information to another corporate employee. Applicant admitted to a deliberate decision not to inform the FSO of his company of the existence and presence of the classified information because of his business decision that the information was needed to expedite the development of a NATO bid proposal, and his rationalization that others did not follow US guidelines in protecting NATO classified information.

However, Applicant was properly briefed by the corporation on US requirements for protecting NATO classified and restricted information; and he had a duty to comply with such procedures. His decision not to comply falls within Guideline K - Security Violations, as noncompliance with security regulations raises doubts about an individual's trustworthiness, willingness, and ability to safeguard classified information. Conditions that could raise a security concern and may be disqualifying include: 2. Violations that are deliberate or multiple or due to negligence. The corporation sent Applicant a letter that he had committed a serious violation and that any subsequent behavior would be cause for termination. Also, his clearance was suspended in April 2001 when the Director of DSS took an interim action suspending his Secret clearance based on Applicant's "willful disregard for security regulations and requirements."

To his credit, both before this incident and subsequent to it, Applicant has had a very successful work record and a favorable reference which indicate partial rehabilitation. However, the mitigation[(9)] standards for security violations require more. While he argues that this incident was isolated in an otherwise unblemished 30-year military and civilian career, the incident shows a pattern of conduct that violated a web of security rules. Since Applicant has not had any access to classified information since the security violation was discovered by the FSO in November 2000, he has not been in a position to subsequently re-establish that he does have a positive attitude towards the discharge of his security responsibilities.

In the light of his knowing failure to make required disclosures to the FSO and to follow the NISPOM and SPP security requirements for NATO classified information on which he had been fully briefed, security concerns persist which raise continuing concerns about his security worthiness. Thus, after considering the Appendix I Adjudicative Process factors and the Adjudicative Guidelines, I rule against Applicant on subparagraphs 1.a., 1.a. (1) through 1.a.(5) incorporated under SOR Paragraph 1.

Personal Conduct

The Government clearly established security concerns over Applicant's personal conduct as Applicant's behavior reflects questionable judgment, untrustworthiness, unreliability, or unwillingness to comply with rules and regulations as discussed above. In addition to the security violation concerns discussed above, Applicant made a "conscious business decision" not to inform the FSO on the improper receipt of this classified information and to retain the information as he was under a tight time constraint to develop the proposal. Not only did he decide to use this information even though he "knew it was wrong," he shared the classified information with a corporate proposal manager, Mr. O, who also needed the information and agreed not to disclose their actions to the FSO.

To rebut and overcome the Government's case, Applicant would have to demonstrate that he has mitigated[(10)] this conduct. His current good work record and favorable corporate reference have to be measured against his knowing and willful failure to disclose required information on his security violation from his FSO which he had a duty to disclose fully. Applicant's current supervisor testified that he believes him to be an honest and trustworthy person as Applicant has access to business sensitive information. This manager has no concerns about Applicant handling it properly.

However, I conclude that it is too soon to conclude that Applicant will meet the high standards expected of those granted access to classified information because of the seriousness and willfulness of his deliberate failure to follow government and corporate security rules. While Applicant's favorable work record is impressive, it cannot erase these serious security concerns caused by his misconduct in failing to follow crucial security procedures on which he had been fully briefed. Hence, after considering the Appendix I Adjudicative Process factors and the Adjudicative Guidelines, I rule against Applicant on subparagraphs 2.a. and 2.b. under SOR Paragraph 2.

FORMAL FINDINGS

After reviewing the allegations of the SOR in the context of the Adjudicative Guidelines in Enclosure 2 and the factors set forth under the Adjudicative Process section, I make the following formal findings:

Paragraph 1. Guideline K: AGAINST APPLICANT

Subparagraph 1.a.: Against Applicant

Subparagraph 1.a. (1): Against Applicant

Subparagraph 1.a. (2): Against Applicant

Subparagraph 1.a. (3): Against Applicant

Subparagraph 1.a. (4): Against Applicant

Subparagraph 1.a. (5): Against Applicant

Paragraph 2. Guideline E: AGAINST APPLICANT

Subparagraph 1.a.: Against Applicant

Subparagraph 1.b.: Against 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 the Applicant.

Kathryn Moen Braeman

Administrative Judge

1. This procedure is required by Executive Order 10865, as amended, and Department of Defense Directive 5220.6, dated January 2, 1992 (Directive), as amended by Change 4, April 20, 1999.

2. According to the FSO report to DSS, Applicant attempted to remove the classification markings as he had to keep the document for his work; however, Applicant denied he did so in his own DSS Statement. (Exhibits 4, 6; TR 61-62) In this DSS Statement Applicant declared that he "never attempted to alter or destroy the classified markings on the CD or paper documents." This violation was not specifically alleged in the SOR.

3. Applicant questioned a DSS agent who testified over whether or not DSS had 'verified" that indeed the information was properly classified, but the agent could not answer that question; the DSS industrial security specialist who handled the investigation had subsequently retired. (TR 47-51)

4. Unauthorized receipt of classified information is a violation of Paragraph 10-401 of the National Industrial Security Program Operating Manual (NISPOM), DoD 5220.22-M (ON I) and of the facility Security Practices Procedures (SPP) Manual dated September 9, 1999 (ON II).

5. While Applicant denied SOR 1.a.(2) in his Answer, he failed to provide any additional proof at the hearing of the basis of his denial which was established by the Administrative Inquiry (AI). This conduct was a violation of paragraph 5-100 of DoD 5220.22-M, NISPOM, January 1995 (ON I)

6. While Applicant insisted in his Answer that the information in the CD-Rom was "readily available in the public domain and had been discussed in Europe in unclassified meetings," he did not offer proof of that position at the

hearing. To buttress his view on others treatment of NATO restricted information, Applicant did provide an affidavit from Mr. W, who had worked with Applicant during the corporation's pursuit of another NATO procurement which explained that others from outside the US operated under less restrictive handling rules for NATO restricted information. (Exhibit A) However, that singular view is not sufficient evidence to establish that the NATO information on the CD was improperly classified or to justify Applicant's deliberate failure to follow the NISPOM and SPP requirements.

7. While Applicant denied SOR 1.a.(3) in his Answer, he failed to provide any additional proof at the hearing of the basis of his denial. Unauthorized processing of classified information in non-accredited Automated Information Systems (AIS) is a violation of Paragraph 8-200(a) of the NISPOM. (ON I)

8. Failure to safeguard classified information is a violation of Paragraphs 5-100 and 5-304 of the NISPOM and of the facility Security Practices Procedures (SPP) Manual dated September 9, 1999. (ONI & II)

9. **Conditions that could mitigate security concerns include actions that:** 1. Were inadvertent;

2. Were isolated or infrequent; 3. Were due to improper or inadequate training; 4. Demonstrate a positive attitude towards the discharge of security responsibilities.

10. **Conditions that could mitigate security concerns include:** 1. The information was unsubstantiated or not pertinent to a determination of judgment, trustworthiness, or reliability; 2. The falsification was an isolated incident, was not recent, and the individual has subsequently provided correct information voluntarily; 3. The individual made prompt, good-faith efforts to correct the falsification before being confronted with the facts; 4. Omission of material facts was caused or significantly contributed to by improper or inadequate advice of authorized personnel, and the previously omitted information was promptly and fully provided; 5. The individual has taken positive steps to significantly reduce or eliminate vulnerability to coercion, exploitation, or duress; 6. A refusal to cooperate was based on advice from legal counsel or other officials that the individual was not required to comply with security processing requirements and, upon being made aware of the requirement, fully and truthfully provided the requested information; 7. Association with persons involved in criminal activities has ceased.