DATE: May 27, 20003

In re:

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

Applicant for Security Clearance

ISCR Case No. 01-13298

DECISION OF ADMINISTRATIVE JUDGE

JAMES A. YOUNG

APPEARANCES

FOR GOVERNMENT

Kathryn D. MacKinnon, Esq., Department Counsel

FOR APPLICANT

H. Lowell Brown, Esq.

SYNOPSIS

Sixty-four-year-old Applicant discovered classified information on a CD he was given so he could work at home. Applicant failed to properly secure or mark the CD or report the security violation to security officials. Applicant informed the project manager who convinced Applicant to keep using the classified materials to complete the project. Applicant failed to demonstrate it is in the national interest to grant him a clearance. Clearance is denied.

STATEMENT OF THE CASE

Applicant, an employee of a defense contractor, applied for a security clearance. The Defense Office of Hearings and Appeals (DOHA), the federal agency tasked with determining an applicant's eligibility for access to classified information, declined to grant Applicant a clearance. In accordance with the applicable Executive Order[(1)] and Department of Defense Directive,[(2)] DOHA issued a Statement of Reasons (SOR) on 19 July 2002 detailing why a clearance was not granted and recommending Applicant's case be referred to an administrative judge to determine whether the clearance should be denied/revoked. In the SOR, DOHA alleged Applicant failed to meet the security violations (Guideline K) and personal conduct (Guideline E) personnel security guidelines of the Directive.

Applicant answered the SOR in writing on 26 November 2002. The case was assigned to me on 7 January 2003. On 29 April 2003, I convened a hearing to consider whether it is clearly consistent with the national interest to grant Applicant's security clearance. The Government's case consisted of six exhibits. Applicant testified on his own behalf, called one other witness, and submitted five exhibits. DOHA received the transcript (Tr.) of the proceeding on 7 May 2003.

FINDINGS OF FACT

Applicant, a 64-year-old international marketing manager for a defense contractor, held a security clearance for many years. In 1999, Applicant's company received a request for proposal (RFP) from a foreign government. The company

responded in October 1999 with information that improperly commingled algorithms that were in the public domain and those that were controlled by the International Traffic in Arms Regulations (ITAR). Ex. 6 at 1; Ex. E at 1. During the internal company discussions concerning the RFP, an issue arose as to whether information in one of the charts was controlled by ITAR. Ex. 1 at 2-3.

[Company] engineers prepared the technical date in the report and as the lead marketing person . . . I along with our technical personnel, reviewed the proposal for any classified information. [Company] personnel and I discussed a chart containing data that was in the proposal. We felt the chart and data was not International Traffic and Arms Regulation controlled if we kept the data in the report. I had final responsibility to approve or disapprove the report, I decided to submit it containing the chart. The report was later reviewed by [the Company] facilities security officer (FSO). She felt that the chart should not have been in the report.

Ex. 1 at 2-3. Applicant apparently failed to get the export administrator (the facilities security officer) to clear the report before transmitting it to the representatives of the foreign government. The company reported an ITAR violation to the U.S. Department of State. The State Department concluded that "a serious infraction had occurred," but determined that the measures taken by the company were sufficient to avoid further sanction. Ex. E at C.[(3)]

In approximately October 2000, Applicant was asked to work on a company project with a short suspense. Tr. 44. He was told that information he would need for the project was on a CD and could be obtained from a co-worker. He obtained the CD, but was unaware there was any classified material on it because it did not contain any security markings. Tr. 53. He took it home to work on over the weekend. Ex. 1 at 1. On Saturday, he inserted the CD into his computer and printed out several of the documents contained on it. *Id*.; Tr. 81. Some of the pages contained NATO Confidential or NATO Restricted markings. Ex. 1 at 1; Ex. C. Realizing that he should not have classified materials in his home, Applicant locked the CD and printed materials in a file cabinet in his home office for the rest of the weekend. Tr. 56. On Monday, Applicant took the printed materials, but not the CD to work. He locked the printed materials in a container authorized to secure classified information, and told the project manager that some of the material on the CD was classified. Tr. 55-57. The project manager told Applicant that he had received the CD through the mail, he had made arrangement to get a document brought in through proper channels, the project was time critical, and Applicant should keep working with it. Tr. 55. Applicant did so. Tr. 59.

Several days later, the company security officer entered Applicant's office, saw what he was working on and asked him about it. Ex. 5 at 4-5. Applicant told her about the CD, explained how he was securing it in his home, and showed her the pages he had printed from the CD. Tr. 60. The security officer told Applicant to bring the CD in. Applicant retrieved the CD from his house and turned it over to the security officer. Tr. 61. The CD was still devoid of any security markings. Ex. C. Applicant was provided with some security software to clean his computer. He did so, but a few days later the security officer had him take the computer to work so it could be checked by experts. Tr. 62. The machine was clear. Tr. 63. Applicant cooperated fully with the investigation that ensued and accepted full responsibility for his actions. Ex. C. The security officer reported the incident to the Defense Security Service as required.

Applicant is a key member of the defense contractor's management team. The chief executive officer and founder of the company believes Applicant has learned his lesson and there will not be a repeat incident. He believes Applicant does not represent a security risk.

POLICIES

"[N]o one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988). As Commander in Chief, the President has "the authority to . . . control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to occupy a position . . . that will give that person access to such information." *Id.* at 527. The President has restricted eligibility for access to classified information to United States citizens "whose personal and professional history affirmatively indicates loyalty to the United States, strength of character, trustworthiness, honesty, reliability, discretion, and sound judgment, as well as freedom from conflicting allegiances and potential for coercion, and willingness and ability to abide by regulations governing the use, handling, and protection of classified information." Exec. Or. 12968, *Access to Classified Information* § 3.1(b) (Aug. 4, 1995). Eligibility for a security clearance is predicated upon the applicant meeting the security guidelines contained in

the Directive.

Enclosure 2 of the Directive sets forth personal security guidelines, as well as the disqualifying conditions (DC) and mitigating conditions (MC) under each guideline. In evaluating the security worthiness of an applicant, the administrative judge must also assess the adjudicative process factors listed in ¶ 6.3 of the Directive. The decision to deny an individual a security clearance is not necessarily a determination as to the loyalty of the applicant. *See* Exec. Or. 10865 § 7. It is merely an indication that the applicant has not met the strict guidelines the President and Secretary of Defense have established for issuing a clearance.

Initially, the Government must establish, by substantial evidence, that conditions exist in the personal or professional history of the applicant which disqualify, or may disqualify, the applicant from being eligible for access to classified information. *See Egan*, 484 U.S. at 531. "[T]he Directive presumes there is a nexus or rational connection between proven conduct under any of the Criteria listed therein and an applicant's security suitability." ISCR Case No. 95-0611 at 2 (App. Bd. May 2, 1996) (quoting DISCR Case No. 92-1106 (App. Bd. Oct. 7, 1993)).

Once the Government establishes a disqualifying condition by substantial evidence, the burden shifts to the applicant to rebut, explain, extenuate, or mitigate the facts. ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002); *see* Directive ¶ E3.1.15. An applicant "has the ultimate burden of demonstrating that it is clearly consistent with the national interest to grant or continue his security clearance." ISCR Case No. 01-20700 at 3. "[S]ecurity clearance determinations should err, if they must, on the side of denials." *Egan*, 484 U.S. at 531; *see* Directive ¶ E2.2.2.

CONCLUSIONS

Guideline K-Security Violations

In the SOR, ¶ 1.a., DOHA alleged under Guideline K that Applicant knowingly and willfully failed to follow security requirements concerning the use and distribution of NATO Confidential information in that he (1) circumventing security regulations by retaining the material at his private residence without approval; (2) failing to physically mark the CD containing the material with appropriate security markings; and (3) storing the materials in a container not approved for retention of such classified information. Under Guideline K, the noncompliance with security regulations raises doubt about an individual's trustworthiness and his willingness and ability to safeguard classified information. Directive ¶ E2.A11.1.1.

Applicant knew that all classified information must be appropriately marked,[(4)] secured in a GSA-approved security container,[(5)] and appropriately protected from inappropriate disclosure. Applicant's noncompliance with security regulations was deliberate. DC 2. He clearly understood that his retaining the classified materials at his home was unauthorized, that he was storing them in an unauthorized container, and that he should have marked the CD with the appropriate security markings. At the hearing, Applicant admitted his derelictions and demonstrated a positive attitude towards the discharge of his security responsibilities. MC 4. He appeared to be remorseful and contrite. However, the weight of such mitigating evidence is tempered by his failure, only a year earlier, to ensure compliance with ITAR on a different project. While the information released on that occasion was not classified, and the release was inadvertent, Applicant was in large part responsible for the violation. Corrective action was taken to make sure future violations would not occur. Apparently Applicant did not learn much from that exercise. Applicant should have been especially sensitive to the need to follow the rules and procedures for protecting classified and sensitive information. Instead, Applicant failed to take the steps required to secure the classified information. The finding is against Applicant.

Guideline E-Personal Conduct

In the SOR, DOHA alleged under Guideline E that Applicant knowingly and willfully failed to follow security requirements for NATO Confidential information as detailed in SOR ¶ 1.a. (SOR ¶ 2.a.) and knowingly and willfully conspired with another to not notify appropriate security officials of the improper receipt of classified information (SOR ¶ 2.b.). Under Guideline E, 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. Directive ¶ E2.A5.1.l.

Applicant's willful refusal to follow the correct procedures in handling and labeling classified information, and his agreement with another employee to continue to violate the security rules, demonstrates his questionable judgment and unreliability. This personal conduct increases his vulnerability to coercion, exploitation or duress. DC 4. It also shows, in conjunction with his failure to handle ITAR materials properly, a pattern of rules violations. DC 5. Applicant took positive steps to significantly reduce or eliminate the vulnerability (MC 5) by causing these materials to be secured only after being confronted by the security officer. The finding is against Applicant.

FORMAL FINDINGS

The following are my conclusions as to each allegation in the SOR:

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

Paragraph 2. Guideline E: AGAINST APPLICANT

Subparagraph 2.a.: Against Applicant

Subparagraph 2.b.: Against Applicant

DECISION

In light of all of 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.

James A. Young

Administrative Judge

1. Exec. Or. 10865, *Safeguarding Classified Information Within Industry* (Feb. 20, 1960), as amended and modified.

2. Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (Jan. 2, 1992), as amended and modified.

3. The SOR did not allege Applicant's participation in the ITAR incident as a basis for denial/revocation of his security clearance. The Evidence of Applicant's culpability in the ITAR violations was not admitted to prove any allegations contained in the SOR, but to determine whether the incident on which the allegations were based was isolated and whether it is likely such behavior will recur.

4. National Industrial Security Program, *Operating Manual* ¶ 4-2-2 (Jan. 1995).

5. *Id.* § 5-304.