DATE: September 8, 2006

In re:

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

Applicant for Security Clearance

ISCR Case No. 04-04264

APPEAL BOARD DECISION

APPEARANCES

FOR GOVERNMENT

Edward W. Loughran, Esq., Department Counsel

FOR APPLICANT

Pro Se

The Defense Office of Hearings and Appeals (DOHA) declined to grant Applicant a security clearance. On August 5, 2005, DOHA issued a statement of reasons advising Applicant of the basis for that decision--security concerns raised under Guideline K (security violations), pursuant to Department of Defense Directive 5220.6 (Jan. 2, 1992, as amended) (Directive). Applicant requested a hearing. On January 12, 2006, after the hearing, Administrative Judge Roger C. Wesley granted Applicant's request for a security clearance. Department Counsel timely appealed pursuant to the Directive ¶¶ E3.1.28 and E3.1.30.

Department Counsel raised the following issue on appeal: whether the Administrative Judge's favorable security decision is arbitrary, capricious and contrary to law and record evidence. Applicant did not file a reply brief.

Whether the Record Supports the Administrative Judge's Factual Findings

A.. Facts.

The Administrative Judge found the following:

Applicant is a 41-year-old senior software engineer for a defense contractor. He had a Top Secret clearance for almost 20 years, and the incident at issue was his sole security violation. The Judge found that Applicant is a senior software engineer who received annual training in the NISPOM.

Late at night, Applicant attempted to log on to an administrator's classified computer, but was unable to do so because access was limited to those with an administrator's password. Applicant then logged on to a colleague's classified computer, and used his personally owned flash memory card with USB adapter (similar to, and referred to hereinafter as, a thumb drive) to download unclassified files. He left the office and went home, where he transferred the downloaded files from the thumb drive to his personal digital assistant (hereinafter PDA) to verify that the files were actually downloaded. Applicant disregarded in-place security procedures without consulting security or system administrator personnel. Applicant disregarded the NISPOM. He neither availed himself of approved trusted downloading procedures, nor checked the PDA for classified information before bringing the device home. He was not sure these downloading actions violated security policy. Then he deleted the downloaded files from the thumb drive and

the PDA.

The next day, the administrator received a message on his computer about needing to reboot when he attempted to log on, disclosing Applicant's attempt to log on the previous evening. As a result of the message on the administrator's computer, later that same day, Applicant was questioned and admitted his conduct as previously described. Upon request, he provided his thumb drive, PDA, and home computer for forensic examination. No classified files were detected. Due to the circumstances of his deliberate security violation, Applicant was sanctioned by his manager. At his hearing, Applicant said his purpose in downloading the files was "to see if the classified computers would recognize and allow access to the memory card device." He had no intention of keeping the unclassified files, only to verify whether or not the procedure would work. Applicant described his actions as an "experiment." He also said it was a "bad decision," and he stated that he should be held accountable for it.

The Administrative Judge found that the security officer was unable to determine if the files were classified or not. He also found that the files Applicant created and downloaded were not classified. The Judge wrote that "inferences warrant . . . that none of the data transferred to Applicant's memory card reader and PDA contained classified information." The Judge also found that Applicant's introduction of the thumb drive and PDA into a DoD closed classified network system without consulting security or system administrator personnel violated paragraph 5-100 of DoD 5220.22-M. Moreover, Applicant had previously received a security briefing where he was told about approved downloading procedures, and that personal computing devices were barred from his facility. Prior to the security violation, Applicant had utilized the proper procedures for downloading unclassified information from a classified computer.

B. Discussion

The Administrative Judge's findings of fact were not explicitly challenged on appeal. However, certain ambiguities and discrepancies are pertinent to the appeal issues raised and are discussed in the conclusions section below.

Whether the record supports Administrative Judge's ultimate conclusions

An Administrative Judge is required to "examine the relevant data and articulate a satisfactory explanation for" the decision, "including a 'rational connection between the facts found and the choice made.'" *Motor Vehicle Mfrs. Ass'n of the United States v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983) (quoting *Burlington Truck Lines, Inc. v. United States*, 371 U.S. 156, 168 (1962)). The Appeal Board may reverse the Administrative Judge's decision to grant, deny, or revoke a security clearance if it is "arbitrary, capricious, or contrary to law." Directive ¶ E3.1.32.3. Our scope of review under this standard is narrow and we may not substitute our judgment for that of the Administrative Judge. We may not set aside an Administrative Judge's decision "that is rational, based on consideration of the relevant factors, and within the scope of the authority delegated to the agency . . ." *Motor Vehicle Mfrs. Ass'n*, 463 U.S. at 42. We review matters of law *de novo*.

The Administrative Judge found that Applicant's conduct was a deliberate security violation. *See* Directive ¶ E2.A11.1.2.2. The Judge concluded that two mitigating conditions were established: (1) the security violation involved a single incident, that is, it was "isolated or infrequent." Directive ¶ E2.A11.1.3.2;.[(1)] and, (2) Applicant " [demonstrated] a positive attitude towards the discharge of security responsibilities. Directive ¶ E2.A11.1.3.4.

Applying a whole person assessment, the Judge concluded: (1) Applicant's explanation for the security violation was extenuating; (2) he provided full disclosure of his security violation; (3) he had an otherwise clean record of observing security procedures; (4) he made positive contributions to his employer's classified software program; and (5) he exhibited remorse, an attitude change, and a renewed understanding about the importance of protecting classified information and abiding by security rules.

Security violations are one of the strongest possible reasons for denying or revoking access to classified information, as they raise very serious questions about an applicant's suitability for access to classified information. ISCR Case No. 97-0435 at 3-4 (App. Bd. July 14, 1998). Once it is established that Applicant has committed a security violation, he has "a very heavy burden of demonstrating that [he] should be entrusted with classified information. Because security violations strike at the very heart of the industrial security program, an Administrative Judge must give any claims of

reform and rehabilitation strict scrutiny." ISCR Case No. 00-0030 at 7 (App. Bd. Sept. 20, 2001). In many security clearance cases, applicants are denied a clearance for having an indicator of a risk that they might commit a security violation (e.g., alcohol abuse, delinquent debts or drug use). Here the issue is not merely an indicator, rather the Judge found Applicant disregarded in-place security procedures in violation of the NISPOM.

Department Counsel asserted that the Judge's determination that the security violation was isolated or infrequent (Directive ¶ E2.A11.1.3.2) and that Applicant demonstrated a positive attitude towards the discharge of security responsibilities (Directive ¶ E2.A11.1.3.4) were not supported by the record evidence. Department Counsel argues that the Judge's acceptance of Applicant's description of his conduct as an "experiment" and his finding of remorse despite Applicant's testimony that the rule prohibiting his conduct was a "grey area" were erroneous. The Judge should have found that Applicant's comments were instead evidence that Applicant did not accept full responsibility for his conduct. (2)

The Judge found that Applicant is a senior software engineer who received annual training in the NISPOM. In short, the Judge's own findings undermine his finding that Applicant "wasn't sure" his downloading actions (from somebody-else's classified computer to his personally owned storage device while working late) violated security policy. Later the Judge refers to the same incident as a deliberate security violation. The Judge then leans back in the other direction when he writes "Applicant's explanations of mishandling his classified computer system, memory card reader and PDA in his possession and control are sufficient to mitigate and extenuate the security violations attributable to him." The Directive instructs that our scope of review shall be to determine whether or not the Administrative Judge's findings of fact are supported by such relevant evidence as a reasonable mind might accept as adequate to support a conclusion in light of all the contrary evidence in the same record. Such is not the case here. The Judge's decision leads the reader in two very different directions about the incident at the heart of the case: it was a deliberate security violation by a man who had to know better, and it was an experiment by a person who wasn't sure what he was doing.

Also troubling is the Judge's statement on page 6 that careful consideration was given to " his absence of any acknowledged classified information in all but two of the incidents. . ." This clause is unclear because it refers to *multiple* incidents and seems to say that *two* of them involved classified information. Previously, he described *one* incident with some ambiguity (3) as to whether there had been *any* classified information involved.

The Judge cites two decisions as Appeal Board guidance. Both decisions are Hearing Office decisions, not Appeal Board decisions, and furthermore are distinguishable from the facts in this case.

Although a Judge has broad latitude and discretion in deciding how to write a decision, the Judge must issue a decision that makes findings and reaches conclusions that the parties and the Board can understand. This is a threshold issue that precedes any analysis of the questions asked by Department Counsel in its brief. Previously, in such cases we have remanded the case *See, e.g.*, ISCR Case No. 02-13568 (App. Bd. Feb 13, 2004) and ISCR Case No. 01-21030 (App. Bd. Jan. 13, 2004). The Board remands the case to the Administrative Judge with instructions to prepare a new decision which is unambiguous, supported by substantial record evidence, and reasonable in light of all the contrary record evidence on the questions of: how many incidents there were, Applicant's level of knowledge of the impropriety of his conduct at the time it occurred, and Applicant's willingness to accept responsibility for his conduct.

Order

The decision of the Administrative Judge granting Applicant a clearance is REMANDED.

Signed: Michael Y. Ra'anan

Michael Y. Ra'anan

Administrative Judge

Chairman, Appeal Board

Signed: Jean E. Smallin

Jean E. Smallin

Administrative Judge

Member, Appeal Board

Signed: Mark W. Harvey

Mark W. Harvey

Administrative Judge

Member, Appeal Board

1. Although only a single allegation is listed in the SOR, and Applicant's conduct occurred on a single night, Department Counsel cited the series of multiple steps involved in accessing, downloading, and transferring the files and contended that the Administrative Judge erred when he did not recognize the seriousness of Applicant's conduct. We disagree. The Judge provided a detailed, step-by-step, description of Applicant's security violation, demonstrating his appreciation of the seriousness of the security violation..

2. *See* ISCR Case No. 97-0625 at 5 (Aug. 17, 1998) (an applicant's refusal to acknowledge his misconduct or accept responsibility for it seriously undercuts a finding that the applicant has mitigated his misconduct). *Cf.* ISCR Case No. 98-0424 at 3 (July 16, 1999) ("An applicant's acknowledgment of the wrongfulness of his or her past misconduct, if found to be credible, has some probative value with respect to a Judge's consideration of whether an applicant has demonstrated reform and rehabilitation. However, an acknowledgment of wrongdoing is merely a first step and does not constitute evidence of conduct that demonstrates reform and rehabilitation.").

3. The Judge found, "[B]ecause the files were deleted from Applicant's memory card reader the [security officer] was unable to determine precisely whether any of the removed data on the memory card was classified or nor."