KEYWORD: Guideline K

DIGEST: The issue in the case is not whether Applicant's security violations were serious, but whether the Judge erred in concluding that they had been mitigated. The Board concludes that the Judge's analysis is rationally connected to his findings. Favorable decision affirmed.

CASENO: 04-04264.a2

DATE: 07/23/2007

DATE: July 23, 2007

|                                     |     |                          |
|-------------------------------------|-----|--------------------------|
|                                     | )   |                          |
| In Re:                              | )   |                          |
|                                     | )   |                          |
|    ----------        | )   | ISCR Case No. 04-04264   |
|                                     | )   |                          |
|                                     | )   |                          |
| Applicant for Security Clearance    | )   |                          |
|                                     | )   |                          |

**APPEAL BOARD DECISION**

**<u>APPEARANCES</u>**

**FOR GOVERNMENT**
Caroline H. Jeffreys, 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) of 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 filed a timely appeal pursuant to Directive ¶¶ E3.1.28 and E3.1.30. This Board remanded the case to the Judge to resolve apparent inconsistencies in his decision. *See* ISCR Case No. 04-04264 (App. Bd. Sep. 8, 2006). On November 22, 2006, the Judge issued a new decision, again granting Applicant a security clearance. Department Counsel has filed a timely appeal to this new decision pursuant to the Directive.

Department Counsel raises the following issue on appeal: whether the Judge's decision is arbitrary, capricious, or contrary to law and the record evidence. Finding no error, we affirm.

**Whether the Record Supports the Judge's Factual Findings**

A. Facts

The Judge made the following findings of fact: Applicant is a senior software engineer for a defense contractor. In March 2003, while working late at his work site, Applicant "experimented" with a memory card transfer procedure on a classified computer. He "wanted to see if he could download unclassified files from his company's classified system to his personally owned USB storage device (or memory card reader) and then check the card through his digital assister (PDA)." Decision at 3. He had previously removed such files, in order to work at home, although utilizing established procedures. He had never previously removed unclassified files from his classified computer using a memory card, and he was not sure he could do it.

Applicant inserted his memory card into the system administrator's personal computer but was not able to log on. He then successfully logged into a colleague's computer, installed his memory card reader, and downloaded unclassified files he had created to he memory card into his PDA. He removed the memory card reader and PDA, secured the area, and went home. The next day he deleted the downloaded files from his memory card reader.

Also on the next day, the system administrator tried to log on to her computer but was not successful. The computer indicated that an unapproved device had been hooked into it and that the administrator should reboot. Subsequent investigation disclosed Applicant's activities in accessing the classified computer system. Forensic analysis confirmed that none of the files Applicant downloaded were classified.

Applicant had been previously briefed on his employer's security policy and NISPOM procedures, including downloading procedures. Applicant's deliberate failure to follow established procedures resulted in his being suspended without pay for one week. Applicant received security refresher training. Applicant has had no prior security incidents or violations. Applicant is highly skilled and successful, credited by his employer as "a model employee since the incident with proven integrity and trust in administering classified systems." Decision at 5.

B. Discussion

The Appeal Board's review of the Judge's findings of facts is limited to determining if they are supported by substantial evidence–"such relevant evidence as a reasonable mind might accept as adequate to support such a conclusion in light of all the contrary evidence in the record." Directive ¶ E3.1.32.1. "This is something less than the weight of the evidence, and the possibility of drawing two inconsistent conclusions from the evidence does not prevent an administrative agency's findings from being supported by substantial evidence." *Consolo v. Federal Maritime Comm'n*, 383 U.S. 607, 620-21 (1966). In evaluating the Judge's findings, we are required to give deference to the Judge's credibility determinations. Directive ¶ E3.1.32.1.

Department Counsel challenges the Judge's use of the term "experimental" in characterizing Applicant's misconduct. Department Counsel argues that this term minimizes the seriousness of Applicant's security violation, as reflected in the record evidence. We have examined the evidence as a whole, however, and conclude that the Judge's use of the word is simply an evaluative judgement drawn from Applicant's testimony and from the exhibits supplied by the Government. We find no basis to question the proposition that Applicant downloaded the files in order to see if it could be done. *See, e.g.*, Gov't. Ex. 2 at 1. The word "experiment" is another way of expressing the same thing. We find no error in the Judge's use of that word in his findings.

**Whether the Record Supports the Judge's Ultimate Conclusions**

A 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 choices 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 general standard is that a clearance may be granted only when 'clearly consistent with the interests of national security.'" *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988). The Appeal Board may reverse the 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 and E3.1.33.3.

In deciding whether the Judge's rulings or conclusions are arbitrary or capricious, the Board will review the Judge's decision to determine whether: it does not examine relevant evidence; it fails to articulate a satisfactory explanation for its conclusions, including a rational connection between the facts found and the choice made; it does not consider relevant factors; it reflects a clear error of judgment; it fails to consider an important aspect of the case; it offers an explanation for the decision that runs contrary to the record evidence; or it is so implausible that it cannot be ascribed to a mere difference of opinion. In deciding whether the Judge's rulings or conclusions are contrary to law, the Board will consider whether they are contrary to provisions of Executive Order 10865, the Directive, or other applicable federal law. *See* ISCR Case No. 03-22861 at 2-3 (App. Bd. Jun. 2, 2006).

We acknowledge that a security violation is a serious matter. Indeed, a person who deliberately violates security rules has breached a fiduciary duty to the United States. *See* ISCR Case No. 97-0435 at 3-4 (App. Bd. Jul. 14, 1998). In the case *sub judice* the issue is not whether Applicant's misconduct is serious, however, but whether the Judge erred in finding it sufficiently mitigated to justify granting him a security clearance.

The Judge concluded that two mitigating conditions operated to Applicant's benefit: that the security violation was isolated or infrequent[1] and that Applicant had demonstrated "a positive attitude toward the discharge of security responsibilities."[2] The Judge stated, "Applicant has exhibited remorse and renewed understanding about the importance of protecting classified information in his custody and control. His avoidance of any other security violations, his contributions to his employer, and his exhibited attitudinal changes are noted. Based on his otherwise good track record for protecting classified information, his expressed remorse, and his avoidance of any recurrent violations in over two years...Applicant carries his evidentiary burden in demonstrating he mitigated the security concerns raised" in the SOR. Decision at 8.

We have examined the Judge's analysis and find it to be rationally connected with his findings. In addition, we conclude that the Judge's analysis is broadly congruent with the record evidence as a whole. We note Applicant's explanation for his motive in downloading the files, that of attempting to broaden his understanding of computer technology. Tr. at 32. That Applicant's stated motive was benign is a factor that weighs in his favor when evaluating the whole person.[3] We also note that his admissions that he exercised poor judgement support the Judge's conclusion as to Applicant's attitude toward his security responsibilities. Tr. at 31, 42. All in all we conclude that the Judge's favorable decision is not arbitrary, capricious, or contrary to law.

**Order**

The Judge's decision granting Applicant a clearance is AFFIRMED.

Signed: Jean E. Smallin
Jean E. Smallin
Administrative Judge
Member, Appeal Board

Signed: James E. Moody
James E. Moody
Administrative Judge
Member, Appeal Board

**DISSENTING OPINION OF ADMINISTRATIVE JUDGE MICHAEL Y. RA'ANAN**

---

[1] Directive ¶ E2.A11.1.3.2.

[2] Directive ¶ E2.A11.1.3.4.

[3] See Directive ¶ E2.2.1 for discussion of whole person factors. Among those listed are "frequency and recency of the conduct"(¶ E2.2.1.3); "presence or absence of rehabilitation" (¶ E2.2.1.6); "motivation for the conduct" (¶ E2.2.1.7); and the "likelihood of continuation or recurrence" (¶ E2.2.1.9).

I cannot concur with the majority. The Judge found that Applicant, a senior software engineer with a defense contractor, had eleven years active duty experience with the Air Force and had regularly serviced classified computer systems. Two and a half years prior to the hearing, Applicant, working late at night, experimented on two other people's computers in order to access a classified system and download files to a personal device.. He then transferred the downloaded files to a second personal device. He then went home with the two personal devices. The Judge correctly identifies this conduct as a deliberate security violation.

The Judge concluded that the deliberate security violation was mitigated. I cannot affirm that conclusion. Applicant was well-informed that what he was doing was prohibited. The fact that he did it late at night, and on other people's computers demonstrates that he engaged in the prohibited conduct in the most surreptitious fashion he could devise, in order to cover his tracks. If no classified information was actually compromised, that is only matter of good fortune. In the Board's first decision in this case we noted that:

> "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.. 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." 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." (Citations omitted).ISCR Case No. 04-04264 at 3-4 (App. Bd. Sep. 8, 2006).

The Judge's decision in this case does not demonstrate that Applicant has met the "very heavy burden" of demonstrating he should be entrusted with classified information.


Signed: Michael Y. Ra'anan
Michael Y. Ra'anan
Administrative Judge
Chairman, Appeal Board