KEYWORD: Guideline K; Guideline M; Guideline E

DIGEST: An applicant who has committed a security violation has a very heavy burden of demonstrating that he should be entrusted with classified information. The evidence from Government Exhibit 2 demonstrates that Applicant engaged in a more extensive pattern of willful security violations than was set forth in the Judge's decision. Favorable decision reversed.

CASENO: 07-08119.a1

DATE: 07/08/2010

DATE: July 8, 2010

In Re:	)	
---	)	ISCR Case No. 07-08119
Applicant for Security Clearance	)	

APPEAL BOARD DECISION

APPEARANCES

FOR GOVERNMENT
Eric H. Borgstrom, Esq., Department Counsel

FOR APPLICANT
Dennis J. Sysko, Esq.

The Defense Office of Hearings and Appeals (DOHA) declined to grant Applicant a security clearance. On July 14, 2009, DOHA issued a statement of reasons (SOR) advising Applicant of the basis for that decision–security concerns raised under Guideline K (Handling Protected Information), Guideline M (Use of Information Technology Systems), and Guideline E (Personal Conduct) of

Department of Defense Directive 5220.6 (Jan. 2, 1992, as amended) (Directive). Applicant requested a hearing. On March 18, 2010, after the hearing, Administrative Judge Marc E. Curry granted Applicant's request for a security clearance. Department Counsel appealed pursuant to Directive ¶¶ E3.1.28 and E3.1.30.

Department Counsel raised the following issues on appeal: whether the Judge's findings of fact were supported by substantial record evidence; whether the Judge erred in denying Department Counsel's motion to amend the SOR; whether the Judge erred in his application of the pertinent mitigating conditions; and whether the Judge's whole-person analysis was erroneous. Finding error, we reverse.

Facts

The Judge made the following pertinent findings of fact: Applicant is a software engineer working for a Defense contractor. He holds a B.S. degree in chemistry.

In 1995 he was reassigned to a different job location, where he remained until 2004. He held a Top Secret clearance with Sensitive Compartmented Information (SCI) access. Applicant's duties included preparing a weekly unclassified report. To do so, he maintained unclassified logs on his program's host computer. He would send the reports to his employer's home office by means of a company computer from his home.

Normally, he would print out a copy of the log and take it home with him. However, in 1998, he took home a disk, inserted it into his company computer, and copied the needed files. He did so because he had grown tired of having to retype the logs at home from the hard copies. This disk, like all of the disks at his workplace, was labeled Secret. He knew that taking the disk home was prohibited and that the security guards would have made him return it if they discovered it as he checked out of his work area. Therefore, he concealed the disk in his pants pocket as he exited. He returned the disk the next day.

Applicant had improperly removed a disk from his workplace on a prior occasion as well. His task was to write an operations manual and, in furtherance thereof, he downloaded two files from a classified computer system onto two disks, took them from his workplace, and loaded them onto his company-issued computer. One of the programs he downloaded was classified. After discovering this, Applicant deleted it from his computer. He reported neither of these incidents to his employer until 2004, after a routine polygraph examination conducted by another DoD agency.

Twice in 2003, and on at least one prior occasion, Applicant removed e-mails with classified banners to his home. Each time he returned them to his workplace and shredded them. Although these incidents were not intentional, he did not report them to his employer.

In 1997, Applicant copied an unclassified phone directory from a coworker's computer without the coworker's knowledge or permission. He noticed that the coworker had left his computer unsecured. He perused the phone directory which was displayed on the computer screen and copied it onto a classified disk, after which he copied it onto his computer. He did not tell his

worker about this, nor did he report the incident until 2004.

In 2003, Applicant inserted a classified disk into a computer classified at a higher level. He did so to spell check a document he needed for a presentation. He failed to write-protect the disk, as required by security regulations.

In February 2004, Applicant was subjected to three polygraph examinations. The following April, Applicants access to SCI was revoked. Since losing his SCI access, Applicant has received counseling regarding security procedures. He had committed only one security violation in the years prior to 1995, the date of his reassignment to the satellite facility.

Applicant enjoys an excellent reputation at work for being security-conscious. In addition, a psychologist who interviewed Applicant concluded that he was "sensitized to security matters." Decision at 8.

Discussion

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 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 general standard is that a clearance may be granted only when 'clearly consistent with the interests of the 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.

Once a concern arises regarding an Applicant's security clearance eligibility, there is a strong presumption against the grant or maintenance of a security clearance. *See Dorfmont v. Brown*, 913 F. 2d 1399, 1401 (9th Cir. 1990), *cert. denied,* 499 U.S. 905 (1991). After the Government presents evidence raising security concerns, the burden shifts to the applicant to rebut or mitigate those concerns. *See* Directive ¶ E3.1.15. The application of disqualifying and mitigating conditions and whole person factors does not turn simply on a finding that one or more of them apply to the particular facts of a case. Rather, their application requires the exercise of sound discretion in light of the record evidence as a whole. *See, e.g.,* ISCR Case No. 05-03635 at 3 (App. Bd. Dec. 20, 2006).

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).

An applicant who deliberately engages in security violations demonstrates a disregard for, or indifference to, national security interests and undermines the integrity and effectiveness of the industrial security program. ISCR Case No. 97-0435 at (App. Bd. Jul. 14, 1998). Once it is established that an applicant has committed a security violation, he has a very heavy burden of demonstrating that he should be entrusted with classified information. Such violations strike at the heart of the Industrial Security Program and the Judge must give any claims of reform and rehabilitation strict scrutiny. ISCR Case No. 00-0030 at 9 (App. Bd. Sep. 20, 2001) *see also Egan*, *supra*, at 527 ("This Court has recognized the Government's 'compelling interest' in withholding national security information from unauthorized persons in the course of executive business.")

Factual Sufficiency

Department Counsel argues that the Judge failed to make findings about and give appropriate consideration to, the findings of a prior Adjudication Board. Thus, the Judge failed to consider an important aspect of the case and, consequently, his decision ran counter to the weight of the evidence.

The Judge concluded that Applicant had mitigated the security concerns in his case, due to his having obtained training on security vigilance and the passage of time since his last infraction.[1] Department Counsel persuasively argues that the Judge's conclusion does not take the full measure of the Government's security concerns about Applicant, citing to record evidence not explicitly referenced by the Judge. He notes evidence contained in Government Exhibit 2, Answers to Interrogatories, dated January 5, 2009, specifically a document from the Adjudication Board which summarized the infractions underlying Applicant's loss of SCI access. Department Counsel persuasively argues that this document paints Applicant's security violations in a less favorable context than is found in the Judge's decision.

Department Counsel's brief quotes liberally from this exhibit. Among the most significant facts contained therein are the following:

During an interview, Applicant "admitted intentionally committing security infractions from 1995 to 2004 to include deliberately removing classified magnetic media and unauthorized material to his home."

"Since approximately 1999, [Applicant] has deliberately concealed misuse of an unclassified [employer-issued] computer located inside of a SCIF. This misuse included surfing the Internet, looking at stock quotes, and buying things. At some point, a coworker mentioned in passing that a security officer had advised that personal use of the computer was unauthorized. [Applicant] deliberately did not follow the guidance provided by the coworker, because he believed it was too rigid and rationalized he did not know what the real policy was, because no one in Security had told

[1]Directive, Enclosure 2 ¶¶ 17(d) and (e); 35(a); and 41(a).

him the policy directly . . ."[2]

"He deliberately did not report security violations, because it is stressful and embarrassing, takes time, and he thought he could get away with it."

"Between 2001 and February 2003, [Applicant] removed unauthorized material from the SCIF once a week . . . He deliberately concealed these violations until confronted with [redacted] polygraph test results . . . During subsequent discussion, he admitted to removing unclassified materials [redacted] on the average of four times a week."

"[H]e recalled that during a bag search a Security Officer found materials with classified banners on one or two occasions that he was unaware of being in his bag. On those occasions, [Applicant] was instructed by the Security Officer to return the material to his office inside the SCIF. When asked if he deliberately disregarded those instructions by purposely concealing the discovered materials on his person prior to exiting the building, he responded that it was possible."

"[Applicant] confirmed the information about deliberately removing unauthorized material between 2001 and February 2004. [Applicant] knew the guards would question him and make him return the material to his office if they found it in his bag, so he purposefully put it in his pockets. [Applicant] knew what he was doing was against facility regulations."

The evidence cited above is, in some particulars, corroborated by Applicant's own evidence at the hearing. However, it differs from Applicant's presentation in that it paints a picture of an ongoing pattern of knowing and willful security violations, in contradistinction to Applicant's contention of merely inadvertent breaches.[3] In doing so, it is corroborated by another document contained in GE 2, a memo for record (MFR) prepared by Applicant's supervisor at the time of his polygraph exams. This MFR describes Applicant as approaching the supervisor on two occasions during the course of the exams and advising about his having taken disks from the workplace and having improperly accessed his coworker's computer to download the phone directory. The tenor of this MFR is that Applicant was, for the first time, admitting to security breaches which he had knowingly committed. There is nothing in this MFR to support or to imply that Applicant was concerned that he was, in response to an aggressive polygrapher, overstating his culpability, as he contended at the hearing. Department Counsel persuasively argues that the cited material from GE 2 constitutes substantial evidence of a more extensive pattern of willful security violations than was

[2]Although not alleged in the SOR, this evidence is relevant in evaluating Applicant's claims of rehabilitation as well as the whole-person factors. *See* Directive, Enclosure 2 ¶ 2(a).

[3]*See, e.g.*, DISCR Case No. 86-3753 at 7-9 (App. Bd. Feb. 28, 1990), for a discussion of deliberate, intentional, or willful conduct in the context of a security violations case. This case states that conduct can be deliberate or willful if "it is voluntary, conscious or purposeful, as opposed to accidental . . . or it involves a careless, reckless or intentional disregard of whether one's conduct is prohibited by law." This case also states that "conduct can be deliberate, intentional or willful even absent any evidence of evil motive or malicious intent."

set forth in the Judge's findings and analysis.[4]

Mitigation

The Judge's conclusion that Applicant had mitigated the security concerns in his case is undercut by record evidence impugning Applicant's credibility. Applicant acknowledged that his hearing testimony was inconsistent with his prior statements in 2004, reflected in GE 2, concerning the willful nature of his security infractions. Tr. at 144. The following inconsistent statements also should have been analyzed by the Judge: GE 2 contains a memo, dated November 5, 2004, signed both by Applicant's attorney and by Applicant himself. This memo was prepared in response to the proposed denial of SCI access. In this document, concerning his removal of the computer disk from the workplace, Applicant stated the following: "[T]here were no guards whatsoever stationed in the part of the factory in which [Applicant] had been working. The only guards on the premises were stationed at the front entrance to the building, and they do not routinely inspect papers or briefcases of people entering or leaving the building." This contradicts Applicant's testimony in which he admitted that the guards searched briefcases and that he concealed the disk in his pants "in order to circumvent security." Tr. at 132.[5]

Another example is Applicant's hearing testimony concerning his failure to write-protect the disk that he inserted into a computer with a higher level classification.

> Judge: So, you deny this, correct?
>
> A: That's correct . . . My contention is I'm–don't know whether I did nor did not write-protect. Tr. at 98-99.

This contention repeats an earlier one contained in the November 5, 2004, memo, in which he stated that he did not recall failing to write-protect the disk. However, only a bit later in the hearing, Applicant, in response to a question by his attorney, admitted to having failed in this responsibility. "Q: You now recall not write-protecting? A: That's correct." Tr. at 106. In admitting that he did indeed fail to write-protect the disk, Applicant contradicted a version of events which he had apparently maintained over a course of years. The Decision does not reflect a thorough examination of Applicant's inconsistent statements regarding a core subject of concern, or the acknowledged overarching inconsistency between his presentation at the hearing with his prior

---

[4]The Judge stated, "Over the years, Applicant negligently removed classified e-mail and intentionally removed unauthorized information from the SCIF." Decision at 9. The substantial record evidence cited by Department Counsel demonstrates that Applicant's security violations were significantly more willful than is suggested by the Judge's use of the term "negligently." While Applicant contended that he never intentionally removed classified information from the SCIF, the evidence cited by Department Counsel points to voluntary, conscious, and purposeful attempts by Applicant to avoid legal strictures designed to protect classified information.

[5]*See also* Tr. at 88: "I never intentionally took out classified information–ever. In terms of taking out a floppy diskette that was marked classified–yes, that occurred around '98." Compare this with Department Counsel's citation from GE 2, above, in which Applicant admitted that it was possible that he had failed to abide by a security guard's instruction to return materials displaying a classified banner to his office.

statements.

We also note another exchange during the hearing, which detracts from Applicant's contention that he had been forthright in describing the actual extent of his security infractions.

> Q: Did you ever put any e-mails in your pants pocket to get past the checkpoint, so the security guards wouldn't actually look at them?
>
> A: I don't recall that. No sir.
>
> Q: Do you recall speaking with any of the investigators, in your different interviews, and admitting having done such?
>
> A: I believe I mentioned about having papers in my pocket. I was asked if I ever had papers in my pocket.
>
> Q: Why would you put papers in your pocket?
>
> A: It was a place to carry them. Tr. at 129.

Such an answer is not credible, in light of other evidence, including Applicant's own testimony immediately subsequent to this exchange, that he knew the guards would search his briefcase but not his pants pocket as he left the building. Tr. at 129-130. The Judge did not discuss the self-serving, and occasionally meretricious, nature of much of Applicant's presentation at the hearing, which seriously impairs his credibility determination and which undermines his overall favorable conclusion as to mitigation.

Applicant's case for mitigation rests on the following contentions, drawn both from the record evidence and from his reply brief. First, he asserted that many of his infractions had occurred after the terrorist attacks of September 11, 2001, when his office was on a war time footing and he was having to work many long hours, resulting in his being tired and in his having cut corners now and then in order to accomplish the mission. Tr. at 79-81. However, the Executive Branch indicated repeatedly in the aftermath of the attacks on the United States that this was a time for increased security vigilance rather than the opposite.[6] Moreover, there is no reason to believe that the stresses Applicant endured in the months and years following September 11 were quantitatively greater than those experienced by countless other contractor personnel who nevertheless managed to avoid security breaches.

Second, Applicant contended that he did not intentionally take classified information out of his workplace and he argued that his infractions were essentially negligent. However, the record and to a lesser extent, the Judge's own findings, viewed as a whole, demonstrate that Applicant exhibited a pattern of willful breaches of security policy, one of which did indeed result in actual removal of

---

[6] *See, e.g.*, Executive Order 13328, Oct. 8, 2001; Executive Order 13231, Oct. 16, 2001; Presidential News Conference, October 11, 2001; Presidential State of the Union, Jan. 29, 2002.

classified information. Applicant's repeated failure to advise his employer of his breaches, and his finally doing so only following three polygraph exams, are consistent with a conclusion that Applicant's infractions were more than excusable negligence.

Third, Applicant noted that he has received counseling on security matters since his last recorded infraction, which he contended impressed upon him the importance of protecting classified and other sensitive data. However, Applicant testified that he received annual security training every year from 1982 until 2004. Tr. at 118. This training clearly did not persuade him to follow the appropriate security requirements during the time alleged in the SOR. Given Applicant's security history, it is not clear from the record or the decision why additional training in the same subject should be viewed as mitigating.

Fourth, Applicant contended that his last infraction occurred in 2004, and that, during the years intervening between then and the date of the SOR, he has had no violations. He argued that he had thereby demonstrated rehabilitation. However, the mitigating force of this evidence is vitiated by the Judge's finding that from March 2006 until October 2007 Applicant did not hold a security clearance at all. In any event, this evidence of good conduct should be balanced against other record evidence demonstrating years of willful security violations accompanied by a deliberate failure to advise his employers concerning them, a failure which Applicant acknowledged was motivated by embarrassment, by wishing to avoid getting into trouble and by his view that reporting them would have been "time consuming." Tr. at 135. The Judge himself acknowledged that the remoteness of Applicant's misconduct, standing alone, is not sufficient to mitigate the security concerns in this case. Decision at 11. We conclude that the mitigating evidence supplied by Applicant or otherwise contained in the record is not enough to pass the strict scrutiny required of security violation cases.

Department Counsel also contends that the Judge erred in denying a motion to amend the SOR. Allegation 2(b) reads as follows: "Between 1994 and 2004, you deliberately misused Government sponsored computers by inadvertently not write-protecting diskettes before using them on a higher security level system and then re-using them on a lower security level system." Department Counsel moved to amend this allegation by striking the words "deliberately" and "inadvertently," thereby avoiding an obvious confusion. Tr. at 263-264. However, the Judge denied the motion. Tr. at 264-265.

The SOR may be amended at the hearing in order to render it in conformity with the evidence, or for other good cause. Directive ¶ E3.1.17. We review a Judge's ruling on a motion to amend for abuse of discretion. ISCR Case No. 06-19544 at 3 (App. Bd. May 28, 2008). Department Counsel's motion was directed at clearing up a flaw in the allegation which, in the Judge's own words, rendered it nonsensical. Decision at 3. By denying a motion to render the allegation intelligible, the Judge undermined his own formal finding on this allegation. That is, on the face of the Judge's decision it is not clear whether he entered his favorable finding due to the nature of the evidence or to the facial defect of the allegation. There would have been no inconsistency in the Judge amending the allegation and then entering a favorable finding based upon the evidence. As it stands, the Judge abused his discretion by not granting Department Counsel's motion or, in the alternative, by not granting Applicant's companion motion to strike the allegation in its entirety.

We have considered the Judge's decision in light of the briefs of the parties and the entirety of the record evidence. The weight of the record evidence demonstrates (as do many of the Judge's findings) that Applicant has repeatedly engaged in willful security violations, which is the very conduct which the industrial security program is designed to prevent. When viewed in light of his inconsistent and otherwise self serving statements at the hearing, the record does not support the Judge's conclusion that Applicant has met his heavy burden of persuasion under Guideline K. Neither does it support the Judge's conclusion that he has met his burden of persuasion under the remaining Guidelines, either as to the mitigating conditions or the whole-person factors. Accordingly, we conclude that the Judge's favorable decision is not sustainable.

Order

The Judge's favorable security clearance decision is REVERSED.

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

Signed: Jeffrey D. Billett
Jeffrey D. Billett
Administrative Judge
Member, Appeal Board

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