KEYWORD: Guideline K; Guideline E

DIGEST: Judge did not abuse his discretion in amending the SOR to conform to the evidence. Applicant's testimony that he did not object to such a procedure waived the issue for purposes of appeal. The Judge properly considered non-alleged conduct in evaluating Applicant's credibility and his case for mitigation. Adverse decision affirmed.

CASE NO: 09-07219.a1

DATE: 09/27/2012

DATE: September 27, 2012

In Re:	)	
	)	
----------	)	ISCR Case No. 09-07219
	)	
	)	
Applicant for Security Clearance	)	
	)	

APPEAL BOARD DECISION

APPEARANCES

FOR GOVERNMENT
Alison O'Connell, Esq., Department Counsel

FOR APPLICANT
Pro se

The Defense Office of Hearings and Appeals (DOHA) declined to grant Applicant a security clearance. On December 8, 2011, DOHA issued a statement of reasons (SOR) advising Applicant of the basis for that decision–security concerns raised under Guideline K (Handling Protected Information) and Guideline E (Personal Conduct) of Department of Defense Directive 5220.6 (Jan. 2, 1992, as amended) (Directive). Applicant requested a hearing. At the hearing, the Judge granted the Government's request to add an allegation under Guideline K. On June 27, 2012, after the hearing, Administrative Judge Juan J. Rivera denied Applicant's request for a security clearance. Applicant appealed pursuant to Directive ¶¶ E3.1.28 and E3.1.30.

Applicant raised the following issues on appeal: whether the Judge erred in his treatment of the disqualifying conditions; whether the Judge erred in his application of the pertinent mitigating conditions; whether the Judge failed to consider all of the record evidence; whether the Judge erred in amending the SOR; whether the Judge improperly considered conduct not alleged in the SOR; and whether the Judge's adverse decision was arbitrary, capricious, or contrary to law. The Judge's favorable findings under Guideline E are not at issue in this appeal. Consistent with the following, we affirm the Judge's decision.

The Judge's Findings of Fact

The Judge made the following pertinent findings of fact: Applicant is a consultant for several Defense contractors. He served in the Army for four years and subsequently in the Federal civil service. He retired from the civil service as a member of the Senior Executive Service (SES) and worked with Defense contractors ever since. He has held a security clearance for many years. He holds Bachelor's and Master's degrees. He has written proposals for Government contractors and is thoroughly familiar with the rules pertaining to security and procurement.

In the late 2000s, a DoD agency sent out a request for proposals (RFP) for the development of a particular type of military equipment. The RFP contained a classified annex. Company A sought Applicant's assistance in preparing a proposal in response to the RFP. Company A sought Applicant's assistance shortly before the proposal was due.

Applicant also had a relationship with Company L. Company L had a facility site clearance but it did not have an information assurance program. Neither did it have authorization to store classified information, although Applicant erroneously believed that it did. Although Company A had applied for a facility clearance, it would not have one before the proposal was due.

Once a company requested the classified annex, the security manager for the requesting agency would review the company's DD Form 254 to ensure that the company had the appropriate clearances and authorizations. Without a DD 254, a contractor could not view a particular contract file, including a classified annex. Applicant was aware of the requirement for a DD 254. Neither he nor Companies A nor L had DD Form 254s on file.

A third company, F, had access to the classified index to the RFP. Applicant went to the premises of Company F to view the annex. He acknowledged that he did so in violation of the rule that requires a DD From 254. Applicant stated that he did so in order to ensure that the proposals he submitted would be in the same format as the annex.

Applicant decided that the proposal needed to go through classified channels. Therefore, he marked his proposal as Secret. He denied that it actually contained classified information, however. He acknowledged that his marking of the document rendered it "presumptively Secret." Decision at 4. His act of doing so was not alleged in the SOR.

Applicant prepared his proposal on a personal computer. The proposal contained information designated as controlled unclassified information (CUI). He acknowledged that doing so was in violation of security rules. Applicant copied his proposal onto several CDs. He placed one CD, marked Secret, in the computer system at Company L. He made two copies of the proposal, leaving one copy at Company L. This copy was marked Secret, although he denied that it actually contained classified information. Because Company L did not have approval to process classified information, it would have been a security violation to download classified information onto one of the company's hard drives.

The SOR contained several allegations of Guideline K violations by Applicant. The Judge concluded that the Government had produced substantial evidence of security concerns regarding two of these allegations: Applicant's having gained access to the classified annex to the RFP without having a required DD Form 254 properly on file and his having used his personally-owned laptop computer to process CUI. As stated above, the Judge resolved all of the Guideline E allegations in Applicant's favor.

The Judge also concluded that Applicant had failed to demonstrate mitigation, citing to evidence of Applicant's lengthy experience with security rules as well as with the requirements of Government procurement. He stated that Applicant knew that he was not complying with security rules in his preparation of the proposal. Although Applicant has made sincere assurances that he will comply with security rules in the future, the Judge concluded that more time was needed to eliminate doubt about his reliability and trustworthiness. In the whole-person analysis, the Judge cited to evidence of Applicant's lengthy service and his positive contributions to national security. He stated that Applicant's admission that he violated security rules is a first step in rehabilitation. Although the Judge expressed confidence in Applicant's ability to comply with security rules, he ultimately concluded that Applicant's conduct raised unresolved questions about his ability or willingness to protect classified information.

Discussion

The Judge's Treatment of the Disqualifying Conditions

Applicant contends that the Judge erred in concluding his conduct in accessing the classified annex met the requirements of Directive, Enclosure 2 ¶ 34(b), in that there is no evidence that he collected or stored classified information in an unauthorized location. Disqualifying Condition 34(b) states that the following could raise a security concern under Guideline K: "collecting or storing classified or other protected information at home or in any other unauthorized location[.]" In the case before us, near the close of the hearing, Department Counsel moved to amend the SOR by adding an allegation that Applicant had violated security protocols by using a personally-owned laptop computer to process CUI. After the Judge granted the motion to amend, Applicant stated to the Judge that he had used his personal computer to process CUI, but that he had done so not on the hard drive but on the computer's random access memory. He explicitly acknowledged the truth of the allegation. Tr. at 374. Insofar as Applicant admitted to having used his personal computer to

draft a proposal that contained CUI, he admitted to conduct that satisfies the requirement of 34(b).[1]

Applicant argues that the Judge erred in concluding that Directive, Enclosure 2 ¶ 34(c) applied to his circumstances. This disqualifying condition addresses "loading, drafting, editing, modifying, storing, transmitting, or otherwise handling classified reports . . . or other information on any unapproved equipment . . ." Although this disqualifying condition does not specifically address CUI, it was not unreasonable for the Judge to consider Applicant's deliberate conduct with CUI under this rubric. Applicant also contends that the Judge erred in applying Directive, Enclosure 2 ¶ 34(f): "Viewing or downloading information from a security system when the information is beyond the individual's need to know[.]" The Judge's findings concerning Applicant's having obtained access to the classified annex without the requisite DD Form 253 are based on substantial evidence and support the application of this disqualifying condition. We resolve this assignment of error adversely to Applicant.

Amendment to the SOR

Applicant contends that the Judge erred in amending the SOR. A SOR may be amended at the hearing in order to render it in conformity with the evidence or for other good cause. We review a Judge's decision to amend the SOR for an abuse of discretion. *See, e.g.*, ISCR Case No. 07-08119 at 8 (App. Bd. Jul 8, 2010). In this case, the evidence adduced at the hearing demonstrated that Applicant placed CUI on his personal laptop, which was in violation of security rules. Applicant admitted that he had done so, as stated above. When Department Counsel moved to amend the SOR, Applicant stated that he did not object and that he did not require additional time in which to prepare to meet the new allegation.

> [Judge]: If I allow the Government to amend, you will have a reasonable period of time to prepare to answer that allegation.
>
> [Applicant]: I don't mind to the amendment, and I don't need any additional time. I'll just answer it now. Tr. at 372-373.

By agreeing to the amendment, Applicant waived any objection he might otherwise have had.[2] Even if he had not waived the issue, given record evidence of the conduct, consisting principally of Applicant's own testimony, the Judge did not abuse his discretion by granting Department Counsel's motion to amend the SOR.

---

[1]To the extent that Applicant is challenging the sufficiency of the Judge's material findings of fact, we note that, in a DOHA case, the Government's burden is to produce substantial evidence regarding controverted allegations. Substantial evidence is "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." Directive ¶ E3.1.32.1. *See* ISCR Case No. 10-10045 at 3 (App. Bd. Jan. 17, 2012). The Judge's material findings of security concern are supported by substantial record evidence.

[2]Applicant raises new evidence in explaining this assertion of error. We cannot consider new evidence on appeal. Directive ¶ E3.1.29.

Conduct Not Alleged in SOR

Applicant contends that the Judge erred by considering evidence that he had knowingly placed a Secret classification designation on documents that contained no classified information. His argument cites to provisions in the NISPOM which, he contends, do not support the Judge's treatment of this evidence. To the extent that Applicant is arguing that the Judge mis-weighed or did not properly evaluate the evidence, he has not demonstrated error. The Judge's finding that Applicant marked unclassified material as though it were classified and that this was improper is supported by the record. See, for example, the testimony of the security manager for the agency that issued the RFP: Applicant stated "that the material was all unclassified . . . If it's unclassified, you don't send a classified document receipt. You don't send it marked secret in packaging marked secret." Tr. at 114.

Moreover, a Judge may consider non-alleged conduct for such issues as an applicant's credibility; his evidence in mitigation; the extent of an applicant's rehabilitation; the applicability of a particular provision of the Directive; or for a whole-person analysis. *See, e.g.*, ISCR Case No. 03-20327 at 4 (App. Bd. Oct. 26, 2006). In the case before us, the Judge stated explicitly that he was considering the non-alleged conduct for these purposes only and for no other purpose. Decision at 5, note 5. We find no error in the Judge's having considered the non-alleged conduct.

Remaining Issues

Applicant contends that the Judge failed to consider various pieces of record evidence. However, a Judge is presumed to have considered all of the evidence in the record. He is not required to discuss every piece of evidence, which is a virtual impossibility in any case. *See, e.g.*, ISCR Case No. 11-00771 at 3 (App. Bd. Apr. 9, 2012). Applicant has not rebutted the presumption that the Judge considered all of the record evidence. Applicant's appeal brief includes evidence from outside the record, concerning, for example, his use of CUI. We cannot consider new evidence on appeal. Directive ¶ E3.1.29.

Applicant cites to statements in the Decision which are favorable to him. He argues that they are inconsistent with the Judge's overall adverse result. We have examined the Decision as a whole, noting several places, especially in the Analysis, in which the Judge cites to favorable aspects of the record, such as Applicant's knowledge, experience, and sincerity. We do not consider individual sentences in isolation; rather, we consider a decision in its entirety. *See, e.g.*, ISCR Case No. 10-03232 at 4 (App. Bd. May 24, 2011). In this case the Judge reasonably explained why the evidence submitted by Applicant was not sufficient to outweigh concerns arising from his failure to comply with rules governing access to classified information and CUI. *See* ISCR Case No. 10-07070 at 8-9 (App. Bd. Apr. 19, 2012) ("Once it has been established that an applicant has committed a security violation, he [or she] 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 . . .").

The record supports a conclusion that the Judge examined the relevant data and articulated 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 Judge's adverse decision is sustainable on this record. "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). *See also* Directive, Enclosure 2 ¶ 2(b): "Any doubt concerning personnel being considered for access to classified information will be resolved in favor of the national security."

Order

The Judge's adverse security clearance decision is AFFIRMED.

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