KEYWORD: Guideline K; Guideline E; Guideline M

DIGEST: The government's witness's testimony was detailed, internally consistent and consistent with other evidence. The fact that the witness discovered no evidence that Applicant was spying does not undermine the legitimacy of the investigation. Applicant's arguments rely on application of an exclusionary rule, which derives from criminal proceedings, and is not applicable in DOHA proceedings, which are civil in nature. Adverse decision affirmed.

CASENO: 10-04911.a1

DATE: 12/19/2011

DATE: December 19, 2011

| | | |
|---|---|---|
| In Re: | ) | |
| | ) | |
| ---------- | ) | ISCR Case No. 10-04911 |
| | ) | |
| | ) | |
| Applicant for Security Clearance | ) | |
| | ) | |

**APPEAL BOARD DECISION**

**APPEARANCES**

**FOR GOVERNMENT**
David Hayes, Esq., Department Counsel

**FOR APPLICANT**
***Pro se***

The Defense Office of Hearings and Appeals (DOHA) declined to grant Applicant a security clearance. On December 22, 2010, 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 E (Personal Conduct), and Guideline M (Use of Information Technology Systems) of Department of Defense Directive 5220.6 (Jan. 2, 1992, as amended) (Directive). Applicant requested a hearing. On September 19, 2011, 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's findings of fact were based upon substantial record evidence; whether the Judge erred in his credibility determinations; whether the Government failed to meet its burden of production; whether the Judge failed to consider all of the record evidence; whether Applicant was denied due process; whether the Judge erred in his application of the pertinent mitigating conditions; and whether the Judge's whole-person analysis was erroneous. Consistent with the following, we affirm the Judge's decision.

**Facts**

The following summarizes the Judge's pertinent findings of fact: Applicant is a Government contractor working for the North Atlantic Treaty Organization (NATO) since the mid-1990s. He served as an officer in the U.S. Army and retired in the mid-1990s. During his career he spent 13 years overseas, including several assignments to NATO. While in the Army, he possessed a top secret security clearance with access to sensitive compartmented information. He had no security incidents while in the Army.

In the mid-1990s Applicant and a partner established a corporation to provide services to NATO countries. He was given a security clearance and, by the time of the hearing, had handled over 300 contracts with NATO.

In early 2007, Applicant attended two meetings in offices inside a NATO building. These meetings were both interrupted by Army counter-intelligence personnel "seeking a rogue wireless transmitter communicating with the embassy of a hostile government from within the NATO building." Decision at 3. Applicant's laptop was identified as the transmitter. He refused permission for investigators to inspect it.

A month later, Applicant turned over his laptop to investigators, who performed a forensic analysis. The analysis disclosed that, over a period of several days prior to turning over the laptop, Applicant had conducted extensive searches for documents containing the words "confidential" and "secret." On one occasion Applicant deleted 200 files from the laptop drive and on another he deleted approximately 2,000.

Applicant backed up his laptop onto an external hard drive before deleting the documents. Investigators recovered 130 of the 2,200 documents that Applicant had deleted, and approximately 100 of them were classified as NATO confidential or above.

Applicant had not registered his laptop with NATO authorities, as he was required to have done. He was not authorized to use a wireless modem from within the building. He registered the laptop with NATO authorities six days after he was asked by investigators for permission to inspect it. The external hard drive was never registered with the proper authorities, and it was not authorized to handle classified documents.

Applicant transferred U.S. and NATO classified documents form his laptop to the external hard drive prior to deleting the documents from the laptop. The external drive was unsecured for approximately 14 months. Although Applicant had a security clearance, he was not authorized to store documents in his laptop, external hard drive, or at his home. During the investigation, he admitted to knowingly loading and storing classified documents in his laptop without authorization.

As a NATO contractor, Applicant was required to update his security clearance annually, to participate in annual security briefings, and to follow appropriate security procedures for the handling of classified information. In August 2005, he signed a document stating that he had been briefed and that he understood the requirements for handling and safeguarding NATO classified information.

Applicant was subsequently arrested and charged with espionage by the host nation government. Authorities searched his house, discovering 38 hard copies of classified documents. He was not authorized to store these documents at his home. After a two year investigation, authorities concluded that there were no hostile foreign intelligence services involved in the incident. Accordingly, the court dismissed the criminal charges.

At the hearing, Applicant stated that, when he had performed the search of his computer, he was surprised to find classified information therein. He stated that most of the documents had been loaded onto his laptop without his knowledge during a one-month deployment. He claimed that, during this deployment, the general officer in charge had authorized him to store NATO confidential documents on the laptop, as a measure of expediency.

After returning from deployment, Applicant did not delete the documents, nor did he notify security personnel that he had documents on his laptop that exceeded the laptop's classification authorization. Applicant's connections with commercial internet providers made the classified information on his computer vulnerable to compromise. At the hearing, Applicant claimed that, at the time of the internet connections, he was not aware that his laptop contained classified information.

Applicant expressed remorse for having stored and possessed the classified information. He intimated that some of the documents were not properly classified and that some of the classifications had been downgraded. However, he presented no corroboration.

He testified that, as result of the criminal and security clearance investigations, he better understands how to handle classified information. His company is training its employees so as to avoid such incidents in the future.

In the analysis, the Judge concluded that the evidence established security concerns under Guidelines K, E, and M. In evaluating Applicant's case for mitigation, he stated that the security violations at issue occurred over a lengthy period of time and, given Applicant's extensive experience as an officer and contractor, such behavior casts doubt on his reliability, trustworthiness, and judgment. The Judge concluded that Applicant's claims about (1) his lack of security training; (2) improper classification of some of the documents; and (3) a general officer having authorized him to place the documents on his computer lacked credibility. He stated that Applicant's security violations were knowing and willful and, given his age, education, and experience, they have not been mitigated. In the whole-person analysis, the Judge made similar statements. He also noted Applicant's attempts to conceal his violations by deleting the files, concluding that these attempts aggravated the seriousness of the conduct.

**Discussion**

Applicant argues that the Judge's findings of fact contained errors. He contends, *inter alia*, that the investigators never found the "rogue transmitter" that they had been seeking, that the favorable resolution of the criminal investigation demonstrated that Government officials had no proper basis to launch an investigation to begin with, that investigators interrupted only one meeting rather than two, etc. However, the record evidence, in particular the investigative summaries contained in Government Exhibit (GE) 3, provides no reason to question the Judge's essential findings of security concern–that Applicant stored classified information on a personal computer without proper authorization and that he attempted to avoid detection by deleting the files before handing the computer over to investigators.[1] *See, e.g.*, ISCR Case No. 09-05399 at 3 (App. Bd. Jan. 11, 2011).

To the extent that Applicant is contending that the Judge failed to consider evidence favorable to him, a Judge is presumed to have considered all of the evidence in the record. *See, e.g.*, ISCR Case No. 10-07080 at 2 (App. Bd. Oct. 12, 2011). Applicant's arguments are not sufficient to rebut that presumption.

Applicant contends that the Judge erred in his credibility determinations. He contends that the Government rebuttal witness, who had conducted the investigation against him, was not competent in the execution of his duties; did not understand significant aspects of the security process, such as the distinction between a security breach and a security compromise; and that his testimony was not worthy of belief.

We have considered this witness's testimony in light of the record as a whole. Contrary to Applicant's assertions, the witness's testimony was detailed and internally consistent, and it was not discredited by cross-examination. It was consistent with other evidence contained in the various investigative summaries provided by the Government. The fact that the witness and his colleagues

[1]*See* Memorandum for DISCO, dated June 26, 2008, contained in GE 3, which states that Applicant's efforts to delete and overwrite the classified files on his laptop made it difficult for investigators to evaluate the full extent of his security violations.

ultimately discovered no evidence that Applicant was spying does not undermine the legitimacy of the investigation itself or of the witness's discharge of his responsibilities. Furthermore, Applicant's arguments rely to an extent on application of an exclusionary rule. Such a rule, which derives from criminal proceedings, is not applicable in DOHA proceedings, which are civil in nature. *See, e.g.*, ISCR Case No. 02-12199 at 6 (App. Bd. Aug. 8, 2005) and ISCR Case No. 97-0184 at 2 (App. Bd. Jun. 16, 1998). At most, Applicant's arguments might affect the weight to be assigned to the Government's evidence. *See, e.g.*, ISCR Case No. 02-05854 at 4 (App. Bd. Apr. 15, 2004).

We also construe Applicant's brief as challenging the Judge's conclusion that Applicant's presentation was, in many respects, not credible. However, this conclusion is based upon a reasonable interpretation of the record. Applicant's testimony was often rambling, and it sometimes veered significantly from the essential issues in the case.[2] Moreover, the record contains evidence of inconsistent statements by Applicant, which also support the Judge's conclusion.[3] In light of the above, Applicant has not overcome the deference owed to the Judge's credibility determinations. *See* Directive ¶ E3.1.32.1. *See* ISCR Case No. 08-01075 at 4 (App. Bd. Jul. 26, 2011).

Applicant also contends that the Government failed to meet its burden of production. In a DOHA hearing, the Government's burden is to present substantial evidence regarding any controverted allegation. 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. 08-06859 at 4 (App. Bd. Oct. 20, 2010). In this case, the Government presented substantial evidence of the security-significant conduct alleged in the SOR. Although Applicant disagrees with the weight which the Judge assigned to the evidence, he has not demonstrated that Judge erred in concluding that the case raised security concerns or in evaluating the case in light of Applicant's burden of persuasion as to mitigation. *See, e.g.*, ISCR Case No. 09-07139 at 2 (App. Bd. Sep. 13, 2011).

---

[2]"[Judge]: I need to interrupt. [Applicant]: Yes, sir. [Judge]: And I want you to concentrate on the issue at hand, which is the documents . . . and how did you get them . . . You have very interesting stories . . . and I would like to hear them, but I want to make sure whether I give you a fair opportunity to tell me . . . how the documents get there, what did you do about them . . . and why I should give you a security clearance." Tr. at 71.

[3]A summary of information contained in GE 3 reflects that Applicant admitted to investigators that he had loaded classified material onto his laptop, stating that he had relied upon his judgment to determine whether the material posed a risk or not. This is not apparently consistent with his testimony that he did not know that the files were on his computer when he had connected to the internet. Tr. at 113. It is also inconsistent with Applicant's response to the SOR, at p. 13, in which he states that NATO personnel transferred classified files to his computer without Applicant's knowledge of the files' classification. The summary of information in GE 3 also avers that Applicant had informed investigators that he had registered his computer when, as they later discovered, he had in fact not done so. We note other support for the Judge's negative credibility determination. Applicant provided no corroboration for his claim that a Belgian general authorized him to store classified information on his personal computer. Moreover, despite evidence of Applicant's having held a clearance for many years and his annual training regarding security matters, he was found to have possessed hard copies of classified documents at his residence without authorization to do so. "Q: You didn't have any sort of approved, under the regulations, intruder detection system, or anything in your home, for classified information? A: I have a . . . guard dog, which I consider to be a pretty formidable counter-intrusion device." Tr. at 155.

Once it is established that an applicant has committed security violations, he or she has a "very heavy burden" of persuasion that he or she should have a clearance. Security violations "strike at the heart of the industrial security program." ISCR Case No. 09-00274 at 2 (App. Bd. Dec. 8, 2010). 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,'" both as to the mitigating conditions and the whole-person factors. *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