

KEYWORD: Guideline K; Guideline M; Guideline E

DIGEST: Judge’s error about Applicant’s age was harmless. The Judge’s material findings were supported by substantial evidence. Applicant failed to rebut the presumption that the Judge considered all of the evidence. Findings and conclusions of a state administrative hearing did not satisfy the requirements for applying the doctrines of *res judicata* or collateral estoppel. The Appeal Board gives deference to a Judge’s credibility determinations. Adverse decision affirmed.

CASE NO: 14-00998.a1

DATE: 03/19/2015

DATE: March 19, 2015

	)	
In Re:	)	
-----	)	ISCR Case No. 14-00998
	)	
Applicant for Security Clearance	)	
	)	

**APPEAL BOARD DECISION**

**APPEARANCES**

**FOR GOVERNMENT**

James B. Norman, Esq. , Chief Department Counsel

**FOR APPLICANT**

*Pro se*

The Department of Defense (DoD) declined to grant Applicant a security clearance. On June 13, 2014, DoD 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 December 22, 2014, after the hearing, Defense Office of Hearings and Appeals (DOHA) Administrative Judge Elizabeth M. Matchinski 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 contained errors; whether the Judge failed to consider all of the evidence; whether the Judge failed properly to weigh the evidence; and whether the Judge's adverse decision was arbitrary, capricious, or contrary to law. Consistent with the following, we affirm.

### **The Judge's Findings of Fact**

Applicant works for a Defense contractor. He held a DoD clearance for ten years prior to being hired by a Defense contractor (Company X). Applicant received periodic briefings on his security responsibilities, including the company's Classification Information Systems Security policy.

In late 2010, Company X issued a security violation alert to all employees. An employee at that company had conducted an unauthorized and improper download using a personal thumb drive, resulting in a contamination of Company X's unclassified network. Employees were advised never to use personal media on any of Company X's systems, classified or not. They were also advised to take their time in performing their duties and avoid rushing. Company X told them to pay attention to classification markings and, if they worked in certain areas, to be knowledgeable about the equipment used, its classification, and permitted operations.

About two months later, Applicant was working in a secure area. He arrived at his duty section around 2:30 a.m., after working long hours the previous day. He needed to transfer classified information from a network at the testing site to a network at another location. Doing so required access to a gateway network, which Applicant did not have. However, another employee (Employee A) had such access. The procedure for transferring classified information was to connect a classified thumb drive to the source network, copy the data, and then upload it to the gateway network by means of a classified personal computer.

On the day in question, Applicant inserted a classified thumb drive into an unclassified laptop computer that was connected to Company X's unclassified network. Doing so was prohibited by the National Industrial Security Program Operating Manual and by policy guidance provided by Company X. Among other things, this guidance stated, "It is a violation of [Company X] policy and [G]overnment security regulations to process classified information on an IS that has not been specifically approved for processing classified information." Decision at 5. The classified thumb drive was conspicuously marked by means of a red tag. Another employee (Employee B) noticed the infraction and removed the thumb drive. Applicant stated to Employee B that he had inserted the thumb drive into the laptop in order to copy a file for transfer to the classified network.

In a subsequent written statement to the Security Manager, Applicant stated that he "accidentally plugged the thumb drive into my laptop USB port." Decision at 6. Based on this statement, and assuming that nothing more of significance would be discovered, the company cleared files from all classified USB drives used to transfer data. However, after this was done, Employee B provided a written statement disclosing Applicant's admission to him that he had

inserted the thumb drive deliberately. When advised of Employee B's statement, Applicant stated that B was lying.

During a meeting with security authorities the next month, Applicant stated that, on the day in question, he had suffered from a sinus headache and was groggy from the effects of medication. He stated that he had not been thinking when he inserted the thumb drive into the laptop and could not explain his actions.

During a meeting the following day, Applicant stated that he had wanted to check unclassified work on his laptop. He demonstrated his actions on the day in question, including that he had accessed the source classified computer before going to his unclassified laptop. Subsequent investigation showed, however, that he had not logged into the source computer. Rather, the computer had been logged in under the credentials of Employee A. Applicant advised that he thought he had logged in to the source computer but that it was possible that he had used Employee A's account. Employee A stated that he did not transfer files for Applicant.

Ultimately, Company X officials concluded that Applicant had knowingly inserted the classified thumb drive into his unclassified laptop. Under the circumstances, classified information was not adequately protected. The company concluded that Applicant had committed a second violation by using the source computer under Employee A's credentials and that Applicant had initially made misleading statements, leading to deletion of evidence during the cleanup process. Company X fired Applicant for "knowingly committing a security violation and repeatedly covering up his actions." *Id.* at 8.

Applicant's claim for unemployment compensation was denied. He appealed that denial, which resulted in a hearing. At the hearing, he claimed that he had not acted deliberately. Ultimately, state authorities overturned the initial denial of unemployment compensation benefits.

The Judge described several other statements Applicant made, including those at his DOHA hearing. He stated that Employee A had moved data to the classified thumb drive at Applicant's request and that Applicant had inserted the thumb drive into his laptop by accident. He stated that his practice of plugging his personal thumb drive into his laptop led him to do the same with the classified thumb drive. When asked why he failed to notice the classified marking on the thumb drive, he stated that the tag was "hanging down on the bottom." *Id.* at 14. He did not recall if he had any other removable media on his desk at the time. He denied telling Employee B that he planned on copying files from his computer on the classified thumb drive. Although he previously had stated that Employee B was lying, at the hearing he surmised that B had merely misunderstood him.

### **The Judge's Analysis**

The Judge concluded that Applicant's conduct raised concerns under each of the Guidelines. She noted Applicant's admission that he had inserted the classified thumb drive into his laptop, denying only that he had done so deliberately. In concluding that Applicant's conduct was indeed

knowing and intentional rather than inadvertent, the Judge cited to evidence that the thumb drive had been clearly marked as classified.<sup>1</sup> She stated that, even if Applicant had been under the influence of medication, his testimony about his other conduct on the day in question did not support a conclusion that he was meaningfully impaired. She also noted both Employee B's contemporaneous statement that Applicant had admitted to him that he had acted deliberately and a lack of evidence that any other thumb drives were present on Applicant's desk for which he could have mistaken the classified one.

In evaluating Applicant's case for mitigation, she noted that he had made inconsistent statements about his conduct, which impaired his credibility. She stated that Applicant had not accepted responsibility for his actions, precluding a finding that the conduct was not likely to recur. The Judge noted that the unemployment compensation hearing had found his conduct to have been unintentional. However, she also noted that such a hearing is not binding on the U.S. Government, which has to resolve doubts about clearance eligibility in favor of national security. Under Guideline E the SOR alleged that Applicant had failed to cooperate with Company X's investigation of his misconduct. She stated that his "documented record of inconsistent statements . . . and his unacceptable tendency" to question the motivations of others "are inconsistent with reform." *Id.* at 22-23.

In the whole-person analysis the Judge noted evidence that Applicant and his team were experiencing time pressures, which could have influenced his conduct. She noted Applicant's testimony that he had not received adequate security training. However, she stated that he had held a security clearance for nearly 20 years, which should have provided him with an understanding of security procedures established for a classified information system.

## **Discussion**

Applicant challenges the Judge's finding that he had deliberately inserted the thumb drive into his laptop, that he used Employee A's credentials for the classified login, and that he had not been cooperative with Company X's investigation. We review a Judge's findings of fact to see if they "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." Directive ¶ E3.1.32.1. When evaluating an applicant's statement of mind, a Judge should consider the conduct in light of the entirety of the record evidence. *See, e.g.*, ISCR Case No. 11-10474 at 3 (App. Bd. Sep. 5, 2014).

Evidence that Applicant had initially admitted deliberate conduct, that the classified thumb drive was clearly marked as such, that Applicant had been briefed by Company X of the need for care in handling classified media, and of his inconsistent statements support her finding of deliberate conduct. Record evidence of Applicant's various inconsistent explanations of his conduct support

---

<sup>1</sup>Evidence shows that the tag on the thumb drive was red in color and measured approximately 3" by 7" in size. Statement of Events by Employee B, dated January 27, 2011, included in Government Exhibit 2, Answers to Interrogatories.

her finding that he did not fully cooperate with the investigation. Moreover, the Judge's findings concerning the prior similar violation two months earlier, about which all employees had been apprised, suggest that Applicant had been on notice of the need for vigilance in handling classified media, thereby diminishing the likelihood of a mere thoughtless error. Applicant has also challenged her finding that he is 64 years old, noting that he is actually 62. This error did not likely affect the outcome of the case. Therefore, it is harmless. Otherwise, the Judge's material findings of security concern satisfy the criteria set forth in the Directive for substantial evidence or constitute reasonable inferences that could be drawn from the record.

Applicant cites to various pieces of evidence, including his experience in holding a clearance, his testimony about the role his fatigue and medication played in his conduct, his denials of wrongful conduct, etc. His argument is not sufficient to rebut the presumption that the Judge considered all of the evidence in the record. *See, e.g.*, ISCR Case No. 14-01509 at 2 (App. Bd. Jan. 20, 2015).

He argues that the Judge did not extend sufficient weight to his unemployment compensation hearing. The Judge made rather extensive findings about this hearing. Her conclusion that its findings are not binding on DOHA is correct.<sup>2</sup> The Judge had an independent duty to evaluate the evidence, to make findings, and to draw conclusions therefrom. Although she considered evidence regarding this hearing, the weight that she extended to it was reasonable. Applicant's presentation of an alternative interpretation of the evidence is not enough to show that the Judge weighed the evidence in a manner that was arbitrary, capricious, or contrary to law. *See, e.g.*, ISCR Case No. 13-00786 at 3-4 (App. Bd. Mar. 28, 2014).

Applicant challenges the Judge's credibility determination, arguing that she did not take into account that others may have lied about him. The Judge made findings about statements that other persons made regarding his conduct, and her weighing of this evidence was reasonable. We find no basis to disturb the Judge's evaluation of Applicant's credibility. *See* Directive ¶ E3.1.32.1 for the requirement that we give deference to a Judge's credibility determination. *See also* ISCR Case No. 12-00609 at 5 (App. Bd. Apr. 4, 2014): "Inconsistent statements can impugn an applicant's credibility[.]"

The Judge examined the relevant data and articulated a satisfactory explanation for the decision. The 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."

---

<sup>2</sup>*See Purter v. Heckler*, 771 F.2d 682 at 690 (3d. Cir. 1985) for a discussion of the doctrine of *res judicata*. Among other things, for a prior hearing to be binding, it must have involved the same parties to the current action. The U.S. was not a party to the unemployment compensation hearing. Similarly, the doctrine of collateral estoppel is not applicable here.

**Order**

The Decision is **AFFIRMED**.

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

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

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