KEYWORD: Guideline K; Guideline M; Guideline E

DIGEST: Security violations strike at the very heart of the industrial security clearance program. Adverse decision affirmed.

CASENO: 14-02447.a1

DATE: 02/26/2015

DATE: February 26, 2015

)
In Re:)
)
----------) ISCR Case No. 14-02447
)
)
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 July 2, 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 Technologies), and Guideline E (Personal Conduct) of Department of Defense Directive 5220.6 (Jan. 2, 1992, as amended) (Directive). Applicant requested a hearing. On December 1, 2014, after the hearing, Defense Office of Hearings and Appeals (DOHA) Administrative Judge Edward W. Loughran 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 denied Applicant due process; whether the Judge's Findings of Fact contained errors; whether the Judge erred in concluding that Applicant's circumstances raised security concerns; whether the Judge erred in his application of the mitigating conditions; and whether the Judge's whole-person analysis was erroneous. Consistent with the following, we affirm the Judge's decision.

The Judge's Findings of Fact

Applicant works for a Defense contractor. He is seeking to retain a clearance that he has held since 2002. Applicant and his father work for this company. Their duties required them periodically to spend time at a remote location, which was far from even the nearest motel. This location had a bank of classified computers that were connected to a classified network. These computers could be accessed by remote logins from other locations. A person had to be authorized for remote login.

In 2012, a secure network was created between Applicant's home location and the remote location. As a consequence, it was possible to conduct a remote login between the two locations. However, Applicant did not have authorization to perform remote logins.

Applicant traveled to the remote location in April 2012, but his father could not due to medical reasons. Applicant created a text file with the IP address of the computer at the remote location, placing it on the secure network. He asked his father to attempt a remote login from the home location. Although the father was able to get the login prompt, he could not log on.

Applicant created a Secure Shell (SSH) key while at the remote location. He used this to create a connection between computers at the home location and at the remote. This achieved the same results as a remote login, though by a means that was not approved. Applicant's had no authorization to do a remote login or use the SSH key. This key established an open connection between the computers. Installing and using the SSH were prohibited.

Company officials discovered the text file that Applicant had created containing the IP address of the computer at the remote location. Prior to the company's discovery of the SSH key, Applicant provided a statement to the effect that his father only attempted the login on the day in April. He stated that he only attempted remote logins between computers at the remote location and had not attempted a login from the home location. He did not mention the SSH key.

Subsequently, company officials discovered the SSH key on a computer used by Applicant and his father. The security manager testified that installing any unauthorized software was a violation of the user agreement signed by Applicant. She testified that Applicant did not have authority to conduct a remote login.

Applicant has consistently maintained that he had authority to conduct remote logins. He asserted that he approached Ms. E, a systems administrator, who added him to the group with authorization. He stated that he asked her if it were possible to perform a remote login from the home location. He claimed that she stated that it was and that if Applicant encountered any problems to let her know. However, Ms. E testified that she did not grant Applicant permission to conduct remote logins. Such requests would have to be done by means of a particular form. She stated that she would not add anyone to the approved group unless she was directed to do so by the security team. She also stated that using an SSH key was not permitted.

In an affidavit to an OPM investigator in late 2012, Applicant stated that he asked Ms. E for remote access and that she added him to the list. He admitted asking his father to attempt a remote login and he also admitted creating and using the SSH key. He stated that he believed that this was permitted.

He provided another affidavit in the middle of 2013. He stated that he asked Ms. E how his father could remotely log in from the home location and that she added him to the appropriate group. In this affidavit he also admitted to creating and using the SSH key. He denied any remote logins after April 2012.

Applicant was required to take remedial security training. He enjoys an excellent reputation for the quality of his work performance, character, trustworthiness, honesty, reliability, etc. His witnesses strongly recommended him for a clearance.

The Judge stated that he considered the possibility that Applicant's conduct was the result of an honest mistake. However, he stated that he found Applicant not the be a credible witness. He found that Applicant had not satisfactorily explained why he needed to create an SSH key if he had authorization to perform remote logins as he claimed. The Judge found that Applicant neither sought nor obtained approval from Ms. E to conduct remote logins and that Applicant intentionally provided false information in his 2012 and 2013 affidavits when he stated that Ms. E had given him authorization.

The Judge's Analysis

The Judge concluded that Applicant's circumstances raised security concerns. He stated that Applicant asked his father to attempt a remote login and created an SSH key without authorization, using the key to conduct a login from the remote location to the home location. He also stated that Applicant had intentionally provided misleading information about his activities when he claimed to have received authorization. In evaluating Applicant's case for mitigation, the Judge concluded that he had not accepted responsibility for his misconduct. He stated that the misconduct was not minor and that it continues to cast doubt upon Applicant's fitness for a clearance.

In the whole-person analysis, the Judge noted Applicant's favorable character evidence and his stable work history. However, he characterized Applicant as having "a problem with honesty and following rules." Decision at 11. He stated that he had questions and doubts about Applicant's fitness for a clearance.

Discussion

Applicant contends that the Judge made improper comments to two of his witnesses. He states that the Judge joked about writing down one of the witness's names to get his "clearance taken away." Appeal Brief at 3, citing to Tr. at 168. He also points to a comment the Judge made prior to another witness's testimony: "We almost never take witnesses' security clearances away. I'm just kidding about that." *Id.*, citing to Tr. at 328. Applicant argues that the Judge's statements intimidated the witnesses, causing one to diminish the forcefulness of his testimony and putting the other "on edge." *Id.*

We have examined these challenged statements by the Judge. The first was in reference to testimony by the witness describing an incident in which company management had implied that the witness had violated security protocols. The gist of the testimony was that the witness had been treated unjustly and, by extension, Applicant had been mistreated as well. The statement by the Judge appears to have been a humorous, if perhaps sarcastic, effort to question the relevance of the testimony.[1] It did not imply disbelief in the testimony or an effort to intimidate the witness. The second appears to have been an effort to put a nervous witness at ease prior to his testimony.[2] We note first of all that Applicant was represented by counsel, who made no objection to either of these statements. In any event, even if a reasonable person could find that these statements did not reflect the proper judicial temperament, there is no reason to conclude that they exerted a harmful effect on Applicant's ability to present his case for mitigation. We have examined the witnesses' testimonies and discern therein no obvious equivocation or any indicia that the witnesses provided testimony that was other than candid. Any error by the Judge was harmless. Applicant was not denied the due process afforded by the Directive.[3] To the extent that this assignment of error implies

[1] The witness testified that he asked a company official the way to the restroom, following the directions the official provided. However, the official later challenged the witness for having walked about unescorted. Judge: "I'm trying not to laugh, but I understand your point. It's bizarre . . . Frankly that's an interesting story but I'm not sure what it has with anything to do with us." Tr. at 167-168. The witness then explained the purported similarity between his incident and Applicant's circumstances. "It could be me accused; it could be anyone . . . [Judge]: All right, let me at it, let me get your name. All right I'm writing it down. Just kidding." *Id.*

[2] A witness apparently entered the hearing room to provide testimony. The Judge stated "Come on in, sir. Good afternoon. Don't be nervous. We almost never take witnesses' security clearances away. I'm just kidding about that." Tr. at 328.

[3] Applicant also notes the following: "[Applicant's] conduct showed poor judgment and an unwillingness to comply with rules and regulations, which raises questions about Applicant's ability to protect classified information. The general concern addressed in [Directive, Enclosure 2] ¶ 15 is also raised. *See* ISCR Case No. 12-01683 at 4 (App. Bd. Jun. 10, 2014)." Decision at 8. Applicant states that he cannot find the cited case in the DOHA website and, as a consequence, he is not able to address any concerns that it may raise. We have not been able to find this case either, and

that the Judge lacked the requisite impartiality, we conclude that Applicant has not met the heavy burden of persuasion required for showing that a Judge was biased. *See, e.g.*, ISCR Case No. 11-13949 at 3 (App. Bd. Sep. 5, 2013).

Applicant challenges some of the Judge's findings. He asserts the Judge erred by finding that he was involved in a remote login and that he established the SSH key without authority. He also asserts that the Judge erred in finding that he had deliberately provided false information during the processing of his application. We examine 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. In evaluating an allegation of deliberate falsification, a Judge should consider the applicant's statements or omissions in light of the entire record." *See, e.g.*, ISCR Case No. 11-14265 at 3 (App. Bd. Aug. 28, 2013). We give deference to a Judge's credibility determinations. Directive ¶ E3.1.32.1.

The record supports the challenged findings. The Government presented documentary evidence that included a report of an inquiry into Applicant's misconduct. The Government also presented testimony by Ms. E, who unequivocally denied having authorized Applicant to proceed as he did. The record, viewed as a whole, contains substantial evidence that Applicant engaged in his security significant conduct without the proper authorization and that his statements to the contrary were deliberately false. The Judge's material findings of security concern are supported by substantial record evidence or constitute reasonable inferences that could be drawn from the evidence. *See, e.g.*, ISCR Case No. 12-03420 at 3 (App. Bd. Jul. 25, 2014).

Applicant contends that his circumstances do not raise security concerns. When an applicant denies an SOR allegation, as is the case here, the Government must produce evidence in support of the allegation. Directive ¶ E3.1.14. The Directive presumes a nexus between admitted or proved conduct under any of the Guidelines and an applicant's security worthiness. *See, e.g.*, ISCR Case No. 11-10255 at 4 (App. Bd. Jul. 28, 2014). The evidence supporting the Judge's findings that Applicant had engaged in a remote login without authorization, established the SSH key without authorization, and made deliberately false statements in the course of his clearance investigation are sufficient to raise concerns under the Guidelines alleged in the SOR.

We find no reason to disturb the Judge's application of the mitigating conditions. The Directive states that an applicant's failure to provide full, frank, and truthful answers to the lawful questions of investigators "will normally result in an unfavorable clearance action." Directive, Enclosure 2 ¶ 15. In addition, once it is established that an applicant has committed security violations, he or she has a "very heavy burden" of persuasion as to mitigation. Such violations "strike at the heart of the industrial security program." ISCR Case No. 11-09219 at 3 (App. Bd. Mar. 31, 2014). Given the record that was before him, the Judge's conclusion that Applicant had failed to meet his burden of persuasion as to mitigation is supportable.

conclude that the citation is likely a typographical error. Insofar as DOHA Judges, including members of the Appeal Board, have no authority to raise concerns other than those that are fairly embraced by the language of the Directive, this error did not impair Applicant's ability to address the Judge's conclusions.

Applicant notes that the Judge did not address each of the whole-person factors set forth in Directive, Enclosure 2 ¶ 2(a). However, a Judge is not required explicitly to discuss all of these factors, and decisions do not turn simply on finding that one or more of them apply to the facts of a particular case. *See, e.g.*, ISCR Case No. 11-08546 at 4 (App. Bd. Feb. 27, 2013). Rather, a whole-person analysis should consider the Applicants conduct in light of the entirety of the record evidence. *See, e.g.*, ISCR Case No. 12-03077 at 2-3 (App. Bd. May 13, 2013). We find no reason to conclude that the Judge's analysis was deficient in this regard.

Applicant cites to language in the summary of his clearance interview to the effect that there is nothing in his background that would subject him to blackmail. However, this merely summarizes Applicant's replies to the investigator's questions. It does not constitute the considered opinion of the investigator. *See, e.g.*, ISCR Case No. 11-05685 at 3 (App. Bd. Jul. 12, 2013).

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."

Order

The Decision is **AFFIRMED**.

Signed: Michael Y. Ra'anan
Michael Y. 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