KEYWORD: Guideline E; Guideline M

DIGEST: In deceiving IT personnel to capture the password and using it without authorization, Applicant repeatedly violated IT security procedures. This put his former employer's IT systems at risk. While he contends he acted in the interest of organizational efficiency, he did so for his own convenience. Adverse decision affirmed.

CASENO: 18-00827.a1

DATE: 03/12/2019

DATE: March 12, 2019

In Re:	)	
	)	
----------	)	ISCR Case No. 18-00827
	)	
	)	
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 May 16, 2018, DoD issued a statement of reasons (SOR) advising Applicant of the basis for that decision—security concerns raised under Guideline M (Use of Information Technology) and Guideline E (Personal Conduct) of Department of Defense Directive 5220.6 (Jan. 2, 1992, as amended) (Directive). Applicant requested a hearing. On November 15, 2018, after the hearing, Defense Office of Hearings and Appeals (DOHA) Administrative Judge Eric H. Borgstrom denied Applicant's request for a security clearance. Applicant appealed pursuant to Directive ¶¶ E3.1.28 and E3.1.30.

Applicant raised the following issue on appeal: whether the Judge's decision was arbitrary, capricious, or contrary to law. Consistent with the following, we affirm.

The Judge's Findings of Fact and Analysis

Applicant is a 39-year-old employee of a defense contractor. He is married with two children and has earned a doctorate degree.

For over three years, Applicant worked in a laboratory. To install hardware or software on his lab computers, he was required to have IT personnel input a password in the computer, and he found these procedure overly protracted. In 2012, he acquired a key-logging device to capture the password surreptitiously. He did not scan the device for viruses or other corruption software. He later captured the password from an IT representative without his or her knowledge. Applicant subsequently used the stolen password on about 12 occasions to install hardware and software onto the lab computer without authorization.

Applicant explained that he circumvented the security procedures in the interest of organizational efficiency. He did not share the password with anyone or install any hardware or software that would have been prohibited. He never received any security training, although he was aware of the procedures for installing hardware or software. He never informed his employer of his use of the key-logging device. He disclosed its use on his 2012 security clearance application (SCA).

Applicant is well regarded by his supervisors, coworkers, and friends. He did not disclose his misconduct to his former employer due to embarrassment. He sincerely regrets his misconduct, but characterizes it as minor.

In deceiving IT personnel to capture the password and using it without authorization, Applicant repeatedly violated IT security procedures. This put his former employer's IT systems at risk. While he contends he acted in the interest of organizational efficiency, he did so for his own convenience. "If his actions were done in the name of organizational efficiency, he would not have acted surreptitiously or felt the need to continue to conceal his past misconduct from his former and current employer. His ongoing concealment of his actions continues his former employer's exposure

to malware, viruses, etc. Applicant's conduct constituted a serious breach of trust and reflected poor judgment." Decision at 4-5.

Discussion

In his appeal brief, Applicant argues the Judge did not fairly weigh the evidence. For example, he contends he had no security training at the time of the alleged conduct; he did not knowingly or intentionally put the former employer's IT system at risk; he engaged in the conduct so that he could do his job more effectively and efficiently; his concealment of the conduct from his former employer did not invalidate his motive; his conduct was minor and, to his knowledge, never harmed the computer system; and he disclosed the conduct on his SCA. He also contends the Judge inadequately applied the whole-person concept by ignoring evidence of his good judgment and character. However, the presence of some mitigating evidence does not alone compel the Judge to make a favorable security clearance decision. A party's disagreement with the Judge's weighing of the evidence, or an ability to argue for a different interpretation of the evidence, is not sufficient to demonstrate the Judge weighed the evidence or reached conclusions in a manner that is arbitrary, capricious, or contrary to law. *See, e.g.,* ISCR Case No. 15-08684 at 2 (App. Bd. Nov. 22, 2017).

Applicant has failed to establish the Judge committed any harmful error. The Judge examined the relevant evidence 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, Encl. 2, App. A ¶ 2(b): "Any doubt concerning personnel being considered for national security eligibility will be resolved in favor of the national security."

Order

The Decision is **AFFIRMED**.

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

Signed: James F. Duffy
James F. Duffy
Administrative Judge
Member, Appeal Board

Signed: Charles C. Hale
Charles C. Hale
Administrative Judge
Member, Appeal Board