KEYWORD: Guideline M; Guideline E

DIGEST: Applicant contends that Department Counsel had a copy of the investigative report before the SOR was issued but did not make that document available to him until he requested a hearing. The record reflects that Applicant was provided a copy of GE 2 in Department Counsel's discovery letter that was sent to him more than six months before the hearing was held. The Directive does not contain any provision that required Department Counsel to provide Applicant a copy of the investigative report when the SOR was issued. Applicant has failed to establish that the due process rights afforded him under the Directive were violated.

Applicant notes that he was never investigated by the Federal Bureau of Investigation or charged with any criminal violation even though some information in the investigative report reflects he engaged in such conduct. He is apparently relying on the lack of a criminal investigation or charges as a basis to argue the former employer's investigative report lacks merit. Even though applicant was not investigated by law enforcement authorities and was never arrested, charged, or convicted of an offense, a Judge may still find the applicant engaged in misconduct that raises security concerns. Adverse decision affirmed.

CASE NO: 18-02592.a1

DATE: 01/06/2021

DATE: January 6, 2021

In Re:	)	
----------	)	ISCR Case No. 18-02592
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 August 30, 2019, 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 December 27, 2019, Department Counsel amended the SOR by adding a Guideline B (Foreign Influence) allegation. On October 7, 2020, after the hearing, Defense Office of Hearings and Appeals (DOHA) Administrative Judge Marc E. Curry denied Applicant's request for a security clearance. Applicant appealed pursuant to Directive ¶¶ E3.1.28 and E3.1.30.

The Judge's favorable findings under Guideline B were not raised as an issue on appeal. The Judge found against Applicant on a single allegation that was cross-alleged under Guidelines M and E. Applicant raised the following issues on appeal: whether the Judge erred in an evidentiary ruling, whether the evidence was sufficient to establish that Applicant violated a former employer's policies, and whether the Judge's decision was arbitrary, capricious, or contrary to law. Consistent with the following, we affirm.

The Judge's Pertinent Findings of Fact

Applicant, who is in his 30s, has earned a bachelor's degree. He has been working in the information technology (IT) field for an number of years and has been working for a defense contractor for the past two years.

In late 2014, Applicant's employer suspected him of suspicious computer activity. The Judge specifically found:

> [A]n analysis of one of Applicant's computers indicated that he attempted to initiate a peer-to-peer connection with a remote host outside his employer's network. This type of activity was prohibited because of its potential to bypass the employer's security measures. (GE [Government Exhibit] 2 at 7) Further review of Applicant's computer use "discovered attempts to obscure Internet activity by using an anonymous proxy that would hide the destination from [the employer's] IT security

systems, as well as frequent visits to questionable download websites as far back as September 2015."[1] (GE 2 at 7) Moreover, Applicant was visiting websites that provided tutorials regarding how to crack passwords and conduct network attacks, and that he had downloaded a copy of pirated software onto the network. (GE 2 at 9) After an investigation, Applicant was terminated for violation of his employer's Internet use policy. (Answer at 1-2)

Applicant admits that he demonstrated bad judgment accessing some of his "personal stuff" on his work computer. (Tr. 58) However, he contends that he visited hacking-related websites for educational and professional development, and that cyber-security experts need to understand how hackers operate in order to defend against them. (Answer at 2; Tr. 56) He characterized this concept as "ethical hacking," and testified that he was earning an online certification in this field while working for his former employer. (Tr. 54) Applicant contends that his employer allowed him to use the office computer for studying and practical assignments related to his certification during down time. Also, Applicant testified that he made a mistake by not memorializing this permission in writing. (Tr. 57-58; 119)

There were occasions on Applicant's job when information technology specialists might need to visit websites related to hacking for research, or download password-cracking software to gain access to a system where a password was lost. These situations were exceedingly rare. (GE 2 at 8) Applicant's employer characterized the volume of hacking-related content combined with the absence of any specific project that required that type of information "disconcerting," and characterized Applicant's behavior as a demonstration of "incredibly poor judgment." (GE 2 at 9) [Decision at 3-4.]

The Judge's Pertinent Analysis

There is no evidence that Applicant misused information technology in the past five years. He has informed subsequent employers of his employment termination, completed security training courses, and is highly respected in his current job. The Judge, however, concluded:

Applicant's violations of his ex-employer's Internet use policy were extremely serious, as they involved visiting websites containing network hacking and password-cracking tutorials. These violations were particularly egregious because Applicant was responsible, in part, with developing malware defenses for his employer. Under these circumstances, his behavior continues to cast doubt on his reliability, trustworthiness, and good judgment, and AG ¶ 41(a) is inapplicable. Given the unusually high volume of visits to inappropriate hacking websites, and in light of

[1] The quoted sentence from GE 2 at 7 does not contain the year "2015." Since GE 2 is dated in January 2015, it is apparent that document was referring to September 2014, vice 2015.

evidence that Applicant attempted to obscure some of his illicit Internet activity, AG ¶ 41(d) also does not apply. Efforts to conceal his conduct show consciousness of guilt, that is, he was aware that his Internet activity was not permitted. In sum, there is limited evidence of mitigating, but in light of the nature and seriousness of the violations, it is insufficient to fully mitigate the security concerns. [Decision at 7.]

Discussion

In his appeal brief, Applicant essentially contends that the Judge erred in admitting into evidence an investigative report from his previous employer laying out Applicant's network activity[2] because it was not authenticated. The investigative report was a portion of GE 2. The Federal Rules of Evidence serve as a guide in industrial security cases. Directive ¶ E3.1.19. Unless the Directive provides otherwise, those rules of evidence may be relaxed to permit the development of a full and complete record. *Id*. The Appeal Board examines a Judge's challenged evidentiary rulings to determine if they are consistent with the Directive and to determine if they are arbitrary, capricious, or contrary to law. *See, e.g.*, ISCR Case No. 15-05047 at 4 (App. Bd. Nov. 8, 2017).

The authentication issue that Applicant is raising on appeal was addressed below. At the hearing, Applicant was represented by counsel who objected to the investigative report on the grounds that it was not authenticated. Initially, the Judge ruled that portions of GE 2 were admissible, but the investigative report in that exhibit (GE 2 at 7-10) was inadmissible. Tr. at 11-19. After Department Counsel later offered into evidence email communications (GE 4-6) regarding GE 2, the Judge withdrew his initial ruling on the investigative report, decided to reserve making a ruling about the admissibility of those pages at that time, and provided the parties the opportunity to submitted additional matters regarding this issue after the hearing. Tr. at 71-78, 88-91, 146-147, and 160-161. In a post-hearing submission, Department Counsel offered another email, admitted into evidence as GE 7, that confirmed the investigative report was from the former employer's internal personnel records. In the decision, the Judge noted that he had admitted pages 7-10 of GE 2 into the record. From our review of the record, we conclude the Judge did not err by admitting the investigative report into evidence.

As a related matter, Applicant contends that Department Counsel had a copy of the investigative report before the SOR was issued but did not make that document available to him until he requested a hearing. The record reflects that Applicant was provided a copy of GE 2 in Department Counsel's discovery letter that was sent to him on January 22, 2020, more than six months before the hearing was held. The Directive does not contain any provision that required Department Counsel to provide Applicant a copy of the investigative report when the SOR was issued. Applicant has failed to establish that the due process rights afforded him under the Directive were violated.

[2] The previous employer was part of another branch of the U.S. Government and not within DoD. The previous employer's investigative report was not a DoD personnel background report of investigation (ROI) that, as set forth in Directive ¶ E3.1.20, would have required authentication.

Applicant notes that he was never investigated by the Federal Bureau of Investigation or charged with any criminal violation even though some information in the investigative report reflects he engaged in such conduct. He is apparently relying on the lack of a criminal investigation or charges as a basis to argue the former employer's investigative report lacks merit. Even though there is no evidence that an applicant was investigated by law enforcement authorities or that he was never arrested, charged, or convicted of an offense, a Judge may still find the applicant engaged in misconduct that raises security concerns. *See, e.g.*, ISCR Case No. 03-04931 at 4 (App. Bd. Jun. 3, 2005). Applicant also contends the investigative report in GE 2 contains unfounded allegations. In this regard, we have previously stated that an employer's decisions and characterizations of events are entitled to some deference. Such deference extends to an employer's internal investigation. *See, e.g.*, ISCR Case No. 18-00496 at 4 (App. Bd. Nov. 8, 2019). It is also noted that the investigation in question was conducted by a Federal court, and there is a rebuttable presumption that Federal officials and employees carry out their duties in good faith. *See, e.g.*, ISCR Case No. 14-02347 at 4 (App. Bd. Aug. 28, 2015). Applicant's challenges to the investigative report are not persuasive.

Applicant argues that insufficient evidence was presented to show that he had knowledge of the former employer's IT rules. This contention is not persuasive. Knowledge may be established by circumstantial evidence. In this case, GE 2 contains a copy of the former employer's Internet Use Policy that Applicant signed in June 2014. That document lists the two specific policies that Applicant's termination letter states he violated. GE 2 at 2. Applicant certified that he had read his employer's internet policy and would comply with it. GE 2 at 6. Furthermore, Applicant worked in the IT field for a number of years before his employment termination. From our review of the record, the Judge's material findings and conclusions of a security concern are based on substantial evidence or constitute reasonable inferences that could be drawn from the evidence. *See, e.g.*, ISCR Case No. 17-02225 at 2-3 (App. Bd. Jun. 25, 2019).

The remainder of Applicant's arguments amounts to a disagreement with the Judge's weighing of the evidence. He argues, for example, that his sole purpose in visiting the questionable websites was for professional development. The Judge noted this claim in his findings of fact. Based on the Judge's conclusions that Applicant violated the former employer's IT policies and attempted to conceal his conduct, it is apparent that he dismissed Applicant's claim that his visits to questionable websites were for authorized purposes. In this regard, it merits noting that we give deference to a Judge's credibility determinations. Directive ¶ E3.1.32.1. None of Applicant's arguments are sufficient to demonstrate the Judge weighed the evidence in a manner that was 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 that 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 E. Moody
James E. Moody
Administrative Judge
Member, Appeal Board

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