**DEPARTMENT OF DEFENSE**
**DEFENSE LEGAL SERVICES AGENCY**
**DEFENSE OFFICE OF HEARINGS AND APPEALS**
**APPEAL BOARD**
**POST OFFICE BOX 3656**
**ARLINGTON, VIRGINIA 22203**
**(703) 696-4759**

Date: January 19, 2022

| | | |
|---|---|---|
| In the matter of: | ) | |
| ---------- | ) | ISCR Case No. 20-02990 |
| Applicant for Security Clearance | ) | |

# APPEAL BOARD DECISION

## APPEARANCES

**FOR GOVERNMENT**
James B. Norman, Esq., Chief Department Counsel

**FOR APPLICANT**
Phillip Stackhouse, Esq.

The Department of Defense (DoD) declined to grant Applicant a security clearance. On February 20, 2021, DoD issued a statement of reasons (SOR) advising Applicant of the basis for that decision—security concerns raised under Guideline K (Handing Protected Information), 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 September 30, 2021, after the hearing, Defense Office of Hearings and Appeals (DOHA) Administrative Judge John Bayard Glendon denied Applicant's request for a security clearance. Applicant appealed pursuant to Directive ¶¶ E3.1.28 and E3.1.30.

Under Guideline K, the SOR alleged that, while employed by a defense contractor, Applicant deliberately downloaded files containing protected information onto a personal external device in about 2018. This single allegation was cross-alleged as the only allegation under Guidelines M and E. In responding to the SOR, Applicant denied the Guideline K and E

allegations and "accepted" the Guideline M allegation but stated his downloading of protected information was not intentional. The Judge found against Applicant on the three SOR allegations.

Applicant raised the following issues on appeal: whether the Government met its burden of proof, whether the Judge erred in his credibility determination and findings of fact, whether the Judge was biased against Applicant, 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 and Analysis**

Applicant, who is in his thirties, has earned two master's degrees and a Ph.D. In 2007, he began working for a defense contractor (Company A) in the information technology field and was granted a security clearance. In 2018, he accepted a position with his current employer and notified Company A of his intent to resign. On his last day of work at Company A in August 2018, Applicant downloaded over 15,000 files onto a personal USB drive. Applicant took the USB drive with him when he departed the company. A few days later, Company A noticed Applicant's unusual downloading activity just prior to his final departure and began an investigation.

In September 2018, Applicant signed a Company A memorandum that advised him he violated the company's policies by downloading files onto his personal USB drive without authorization. As instructed, he returned the USB drive to Company A. The company later issued an internal memorandum that revealed over 15,000 files totaling over 8 gigabytes were recovered from the USB drive. The memorandum further indicated "Allegation: Data Exfiltration with CI/CT [Counterintelligence/Counter Terrorism] nexus (SUBSTANTIATED)[.]" Decision at 3, citing Government Exhibit (GE) 3 at 1. In October 2018, an adverse information report was filed against Applicant.

In a 2019 background interview, Applicant initially denied he had previously misused information technology before being confronted with Company A records reflecting he was ineligible to be rehired due to the downloading incident. During that interview, he admitted that he accidentally downloaded Company A proprietary information while attempting to download his personal files. At the hearing, he claimed the interview was the first time he learned Company A considered the downloading of the files improper activity. He testified at his hearing that he had Company A's approval to transfer files using a USB drive between the company's two networks and that the company did not require him to use an approved USB drive. He further testified that he used his company laptop for both work and personal purposes. He acknowledged that he was aware he could not take Company A proprietary information when he resigned from the company. He attributed this downloading mistake to haste in retrieving his personal files.

> The nature, extent, and seriousness of his conduct speaks for itself. The fact that he did not seek his employer's prior approval to copy files onto the USB Device strongly suggests that he knew that such approval would be denied or highly supervised. I also found Applicant's testimony and demeanor while testifying to lack credibility on the issue of whether his actions of copying thousands of files from his employer's computer network, some of which contained [Company A proprietary information], was inadvertent. I conclude Applicant knew better and

> was seeking to do something without his employer's approval while hoping he was acting "under the radar" of his employer in the afternoon of his very last day of work there. Unfortunately for Applicant, [Company A's] computer system detected his unusual activity of downloading of large number of files, and an investigation ensued. [Company A] investigators found that their counterintelligence and counterterrorism concerns were substantiated. [Decision at 13-14.]

Some mitigating conditions were partially established; others were not established. Applicant failed to mitigate the alleged security concerns. Overall, the record evidence raises doubt about Applicant's eligibility for a security clearance.

**Discussion**

Deliberate Downloading of Files and Credibility Determination

A central theme running throughout Applicant's appeal brief is that the Judge erred in concluding that Applicant deliberately downloaded the files in question. As a related matter, he also claims the Judge's credibility determination is flawed. These arguments are not persuasive.

Applicant contends that the downloading of Company A's protective information onto his personal USB drive was inadvertent[1] and that insufficient evidence exists to show otherwise. The Judge did not accept those claims. It is well established that circumstantial evidence may prove an applicant's state of mind at the time he or she engaged in a certain act. *See, e.g.*, ISCR Case No. 18-02592 at 4 (App. Bd. Jan. 6, 2021). *See also*, DISCR OSD Case No. 90-0095 at 4-5 (App. Bd. Jan. 14, 1991) (circumstantial evidence may be as probative as direct evidence). The entire record should be examined in making a state-of-mind determination. The relevant factors to consider in making such a determination, of course, depend upon the facts of the case, but frequently include an applicant's age, education, position, experience, as well as the nature, extent, and seriousness of the conduct in question, the circumstances surrounding that conduct, and the plausibility of an applicant's explanation regarding it.

In this case, pertinent facts support the Judge's conclusion that Applicant's downloading of the files was deliberate. First, the downloading at issue occurred on Applicant's last day of employment at Company A. Understandably, an employee's downloading of a large number of files just prior to walking out the door for the last time raises concerns. Another significant fact in this case is Company A's conclusion that Applicant's use of the personal USB drive violated its policies. Its memorandum states:

> A [Company A] investigation has found evidence indicating that [Applicant has] downloaded [Company A] Information to an unauthorized personal electronic

[1] Negligent handling of protected information can raise security concerns and may be disqualifying. *See* Directive, Encl. 2, App. A ¶¶ 33 and 34. In the decision, the Judge stated, "Moreover, his [Applicant's] actions standing alone, without regard to his intent, cast doubt on his current reliability, trustworthiness, and judgment." Decision at 10. Nonetheless, since the SOR alleged, and the Judge found, the downloading of the files was deliberate, this decision will focus on that aspect of the case.

> device or storage media, or connected such devices to [Company A] information systems in violation of Corporate Information Protection Manual Sections [A], Storage of Information on Personally-owned Information Technology Assets and [B] Connectivity of Personally owed information Technology Assets to [Company A] Infrastructure. [GE 3 at 2.]

Conversely, Applicant contends that he was authorized to transfer Company A files between networks using an external hard drive. Tr. at 22-28, 57-66, and 71-78. However, he has not corroborated his claim that the company's authorization for him to use an external hard drive extended to him using a personal USB drive to transfer files from the company's computer system. *Id.* During his testimony, he acknowledged he needed the company's permission to transfer his personal files, although he claimed he was unaware of that requirement when he made the transfer. *Id*. at 26-27. Notwithstanding Applicant's testimony, the above quote from the Company A memorandum provided the Judge a sufficient basis to conclude Applicant was not authorized to connect his personal USB drive into the company's computer system. In this regard, it merits noting the Appeal Board gives deference to a company's findings and conclusions in its security investigations. *See, e.g.*, ISCR Case No. 15-08385 at 4 (App. Bd. May 23, 2018) ("[B]ecause of the unique position of employers as actual administrators of classified programs and the degree of knowledge possessed by them in any particular case, their determinations and characterizations regarding security violations are entitled to considerable deference, and should not be discounted or contradicted without a cogent explanation."). In this case, the Judge committed no error in relying on Company A's report to conclude that Applicant's downloading of the files to his personal USB drive violated the company's policies and that his misconduct was substantiated.

Moreover, Applicant's inconsistent or implausible statements regarding this incident undercut the believability of his claims. For example, his claim that he was unaware at the time that his actions were in violation of company policy is dubious. Tr. at 26-27, Decision at 10, Appeal Brief at 12. The evidence reflects that he is highly educated and worked for Company A for about 11 years. At that company, he held positions as a systems engineer and as an information assurance engineer. Tr. at 20 and GE 1 at 18. At the hearing, he testified that he was required to be aware of how to use USB devices "properly or improperly[.]" Tr. at 20. Given his background and experience as an information technology professional, he should have been well aware of the dangers involved in the downloading of files from the company's computer. It was reasonable to expect that a professional with his background would have taken appropriate steps to safeguard protected information and to conclude that his downloading of the company's proprietary information was deliberate. As the Judge stated, "Even a non-expert employee would readily understand the security risks presented by plugging a privately purchased USB device into the employer's computer network and copying files without the employer's permission." Decision at 13.

In challenging the Judge's credibility determination, Applicant notes that he wore a mask during the hearing[2] and refers to the Judge as a "human lie detector." Appeal Brief at 2, 11, and 19. *See also* Tr. at 18-19. Directive ¶ E3.1.32.1 provides that the Appeal Board shall give deference to a Judge's credibility determination. Additionally, a party challenging a Judge's credibility determination has heavy burden on appeal. *See, e.g.*, ISCR Case No. 02-12199 at 3

[2] The wearing of masks was required to protect against the spread of the COVID-19 virus.

(App. Bd. Aug. 8, 2005). In this case, the Judge had the opportunity to personally observe Applicant's demeanor during his testimony despite the mask and to weigh his testimony in light of the record evidence as a whole. Key considerations in assessing credibility include whether the witness's testimony is contradicted by other evidence or whether it is so internally inconsistent or implausible on its face that a reasonable fact-finder would doubt it. In addition to the contradictions in Applicant's statements noted in the previous paragraphs, the Judge also noted that Applicant initially denied during his background interview that he previously misused any information technology system despite having received Company A's memorandum regarding a violation of its information technology policies. Furthermore, although documentary evidence confirmed that he was informed of those violations prior to his background interview, he continued to claim at the hearing that the background interview was the first time he learned Company A considered the downloading of the files as improper conduct. Tr. at 38-40.

Record evidence supports the Judge's challenged conclusions. Applicant has failed to establish the Judge's conclusion as to Applicant's intent or credibility determination were arbitrary, capricious, or contrary to law.

Findings of Fact

Applicant contends the Judge's findings of fact are not support by substantial evidence. For example, he points out the Judge erred in making a finding regarding the title of his position at Company A. Regarding this matter, the Judge apparently confused Applicant's most recent position title with his former position title at Company A. GE 1 at 17-18. From our review of the record, Applicant has not cited any error in the Judge's findings that would likely affect the outcome of the case. *See, e.g.*, ISCR Case No. 19-01220 at 3 (App. Bd. Jun. 1, 2020).

Mitigating Conditions and Whole-Person Factors

Applicant contends the Judge improperly assessed and weighed the evidence. He argues the Judge erred in concluding that certain mitigating conditions did not apply or others only partially applied. He further asserts the Judge erred in assessing the whole-person factors. In making these arguments, Applicant highlights evidence supporting the application of those conditions or factors. These arguments are not convincing. The presence of some mitigating evidence does not compel the Judge to make a favorable security clearance decision. As the trier of fact, the Judge has to weigh the evidence as a whole and decide whether the favorable evidence outweighs the unfavorable evidence, or vice versa. 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. 19-01431 at 4 (App. Bd. Mar. 31, 2020).

Bias

Applicant contends that the Judge's findings and conclusions denying him a security clearance were biased. Appeal Brief at 3, 6, 7, and 12. He also asserts the Judge's analysis, which he claims was unsupported by facts, impugns his character. Appeal Brief at 9. Neither adverse

findings or conclusions nor an unfavorable decision, standing alone, establish judicial bias. *See, e.g.*, *Bixler v. Foster*, 596 F.3d 751 at 762 (10th Cir. 2010). There is a rebuttable presumption that a Judge is impartial and unbiased, and a party seeking to overcome that presumption has a heavy burden of persuasion. *See, e. g*., ISCR Case No. 18-02722 at 5 (App. Bd. Jan. 30, 2020). Applicant has not directed our attention to anything in the record that would likely persuade a reasonable person that the Judge was lacking in the requisite impartiality.

Conclusion

Applicant failed to establish that the Judge committed any harmful error or that he should be granted an exception under Directive, Encl. 2, App. C. The Judge examined the relevant evidence and articulated a satisfactory explanation for the decision. The decision is sustainable on the record. "The general standard is that a clearance may be granted only when 'clearly consistent with 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 national security."

## Order

The decision is **AFFIRMED**.

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

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

Signed: Moira D. Modzelewski
Moira D. Modzelewski
Administrative Judge
Member, Appeal Board