

Date: January 24, 2023

In the matter of:)	
)	
)	
-----)	ISCR Case No. 21-00363
)	
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 30, 2021, DoD issued a statement of reasons (SOR) advising Applicant of the basis for that decision—security concerns raised under Guideline K (Handling Protected Information) and Guideline E (Personal Conduct) of Department of Defense Directive 5220.6 (Jan. 2, 1992, as amended) (Directive). Applicant requested a hearing. On November 25, 2022, after the hearing, Defense Office of Hearings and Appeals (DOHA) Administrative Judge Eric C. Price 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 and whether the Judge’s adverse decision was arbitrary, capricious, or contrary to law insofar as it ran contrary to the weight of the record evidence. Consistent with the following, we affirm.

The Judge's Findings and Analysis

Applicant is in his mid-50s, married, and has two adult children. He holds bachelor's and master's degrees and has worked for Federal contractors since mid-1990, supporting the same DoD agency for over 20 years. Applicant has held a security clearance since the late 1980s.

From about 1999 until March 2020 Applicant maintained a spreadsheet containing personal privacy information, which he routinely transferred between his Government and personal computers via a USB drive or emails. From at least 2015 until 2020, the spreadsheet also included DoD protected information: access information for a Government safe, personal identification numbers (PINs) for facility access, PINs for access to classified and unclassified IT networks, and the PIN for his DoD ID card. Regarding the safe, Applicant's spreadsheet contained the word "Safe" followed by a six-letter passcode that could be converted to the combination. The last time that Applicant engaged in this conduct was March 2020, discovery of which prompted an investigation into possible spillage of protected information.

When questioned about his activity, Applicant stated that he had transmitted the protected information in March 2020. He did not initially disclose that he had done so over 200 times since 2015. The inquiry substantiated that Applicant had improperly transmitted protected information, some of which was classified. An insider-threat security official testified at the hearing that Applicant's network PIN was determined to be classified, and that the PIN for the DoD agency door, Applicant's ID card, and the safe passcode were "sensitive DoD information." Decision at 7, citing Tr. at 86, 96-99.

In the analysis, the Judge noted the extent of Applicant's security-significant conduct, his training on the proper handling of protected information, and evidence of inconsistent statements concerning this matter. Under Guideline E, the Judge concluded that, in responding to those investigating the spillage, Applicant deliberately minimized his conduct. "[T]he record as [a] whole reflects that from at least 2015 to March 2020 Applicant maintained and updated protected DoD information in a spreadsheet that he routinely transmitted between his DoD email and personal email accounts and that those actions contradicted written statements he provided to DoD security officials[.]" Decision at 11-12. He stated that he found Applicant's explanations to be lacking in credibility. Among other things, the Judge cited to evidence that Applicant acknowledged that he had considered disclosing the full extent of his conduct but did not do so because "it was not correct to bring in a new 'broader' email concern." Decision at 12, quoting AE L at 3.

Discussion

Applicant challenges the Judge's findings of fact. We examine a Judge's findings 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.

Applicant denies that he intentionally transmitted classified information to his unclassified personal email account. The challenged statement, contained in the analysis portion of the

Decision, reads as follows: “The Government presented substantial, un rebutted evidence that the spreadsheet contained classified information including documentary evidence that it contained unspecified classified information, and testimony that Applicant’s classified IT network PIN was classified information.” Decision at 8. This statement is supported by the Incident Summary and by the testimony of the security official. Government Exhibit (GE) 2 at 2; Tr. at 85-86. In his security clearance application, Applicant also disclosed he mishandled classified information by stating, “I stored and sent classified information within an unclassified email environment” in April 2020. GE 1 at 13 and 39. The Judge did not err in finding that the transmissions that Applicant made over the course of several years contained information that was classified. Regarding Applicant’s state of mind, the SOR did not allege nor the Judge explicitly find that Applicant acted with the specific intent to compromise classified information. Rather, the SOR and the Judge’s findings underscore the improper nature of Applicant’s conduct, which is consistent with the record.

Applicant denies that he intentionally sought to mislead investigators as to the scope of his security-significant conduct. He stated that in his initial response to their inquiries he believed that they were only concerned with the events of March 2020 and that when he realized that they were looking into his prior behavior he was properly forthcoming. The allegation to which the challenged finding is directed is as follows:

Between 2015 and 2020, you routinely made updates to sensitive [agency] information in the file you sent between your Government and personal email accounts, including the [agency] passcode in 2017. These actions contradicted the written statements you made to security officials during the investigation of this incident. [SOR ¶ 2c.]

We note first of all that the record does not contain the actual questions posed by the officials nor Applicant’s written replies. However, Applicant does not deny that his initial response was limited to his conduct in 2020 and did not address his entire history of transmitting Government information to his private email account. His position has consistently been that his initial response was not a deliberate effort to mislead but was simply an effort to answer the question asked.

The record contains evidence that undermines this contention: (1) Applicant’s conduct was of longstanding duration; (2) he updated and changed Government information over the course of his conduct (Tr. at 89); (3) he has received periodic training on handling protected information from which he knew or should have known that his conduct was improper; (4) he has worked for Federal contractors and held a clearance for decades, which also should have placed him on notice that his conduct was improper; and (5) he admitted that he considered that the Government could be concerned about his “long term transferring” of files but decided that “it was not correct to bring in a new ‘broader’ email concern.” Applicant Exhibit L, Statement by Applicant, at 3. On this last point, the fact that Applicant’s conduct was of many years’ duration was not a new concern but was squarely within the scope of the investigation at issue. That Applicant deliberated about this matter and chose a more limited response undermines his contention of honest mistake. In addition, we note the Judge’s adverse credibility determination, to which the Directive requires us to give deference. Directive ¶ E3.1.32.1. Taken together the record supports the challenged

finding. A person holding a security clearance has a duty to fully disclose conduct of security concern when asked, and the record supports a conclusion that Applicant failed in this regard. *See, e.g.*, ISCR Case No. 06-11898 at 3 (App. Bd. Dec. 26, 2007).

Even if the Judge erred in this finding, however, it did not likely affect the overall outcome of the case. Given the extent and seriousness of Applicant's improper transmission of protected information, had the Judge found in Applicant's favor concerning any willful act of full disclosure he would still have denied Applicant a clearance. Therefore, any error in the challenged finding was harmless. *See, e.g.*, ISCR Case No. 19-03640 at 3 (App. Bd. Nov. 1, 2022). Applicant has cited to no harmful error in the Judge's findings. The material findings of security concern set forth in the Decision are supported by substantial evidence. *See, e.g.* ISCR Case No. 18-02581 at 3 (App. Bd. Jan. 14, 2020).

Applicant cites to his having served the Government agency for many years. He also testified the spreadsheet that he was emailing to and from his personal computer contained sensitive Government information. Tr. at 49-50. Again, the gravamen of the case is that Applicant improperly transmitted protected Government information, including classified information, over a number of years. The Judge did not rely upon a conclusion that Applicant intentionally failed to protect classified information but that his conduct overall raises serious questions about his judgment and reliability. Security infractions "strike at the heart of the industrial security program" and require strict scrutiny. ISCR Case No. 14-05127 at 9 (App. Bd. June 24, 2016). Applicant's arguments are not sufficient to demonstrate that the Judge weighed the evidence in a manner that was arbitrary, capricious, or contrary to law. *See, e.g.*, ISCR Case No. 18-02872 at 3 (App. Bd. Jan. 15, 2020).

The Judge examined the relevant evidence and articulated a satisfactory explanation for the decision. Applicant has cited to no harmful error in the Judge's findings or analysis. 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: 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 Modzelewski
Moira Modzelewski
Administrative Judge
Member, Appeal Board