DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 18-01025
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Aubrey De Angelis, Esq., Department Counsel
For Applicant: *Pro se*

11/25/2019

_____

Decision

_____

NOEL, Nichole L., Administrative Judge:

Applicant contests the Defense Department's intent to revoke his eligibility for access to classified information. Applicant transferred over 93,000 files containing proprietary information to personal storage devices in the weeks before he started a job at a competing company. He then made false statements to his former employer during the investigation of the issue. Clearance is denied.

Statement of the Case

The Department of Defense Consolidated Adjudication Facility (DOD CAF) issued a Statement of Reasons (SOR) detailing security concerns under the use of information technology (IT) and personal conduct guidelines on May 2, 2018. The DOD CAF took this action under Executive Order (EO) 10865, *Safeguarding Classified Information within Industry*, signed by President Eisenhower on February 20, 1960, as amended; as well as DOD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program*, dated January 2, 1992, as amended (Directive), and the *Adjudicative Guidelines for Determining Eligibility for Access to Classified Information*, implemented on June 8, 2017. Based on the available information, DOD adjudicators were unable to find that it is clearly consistent with the national interest to grant Applicant's security clearance and recommended that the case be submitted to an

administrative judge for a determination whether to revoke or deny Applicant's security clearance.

Applicant answered the SOR on May 21, 2018, and requested a decision without a hearing. The Government submitted its written case on March 11, 2019. A complete copy of the file of relevant material (FORM) and the Directive were provided to Applicant. He received the FORM on March 15, 2019, and provided a response. The attachments to the FORM are admitted to the record as Government's Exhibits (GE) GE 1 through 11, and Applicant's response to the FORM is admitted as Applicant's Exhibit (AE) A, without objection.

Findings of Fact

Applicant, 60, has worked for his current employer, Company A, a federal contracting company, since March 2016. He worked for his previous employer, Company B, another federal contracting company, for 31 years from 1988 until February 2016 when he was ordered to resign in lieu of termination. On February 23, 2016, Company B filed an adverse information report in the Joint Adjudication Personnel System (JPAS), alerting the DOD CAF that Applicant attempted to retain Company B propriety information related to his employment without authorization, and that he made deliberately false statements to a Company B investigator. Applicant completed a security clearance application in August 2016, disclosing that he was disciplined by Company B for having "backup disks that contained company proprietary information." He disclosed that after resigning and providing two-weeks' notice, that Company B released him two days early, informing him by letter after the fact that he resigned in lieu of termination. According to the August 2016 security clearance application, the DOD granted Applicant security clearance eligibility in 2013. It is unclear from the record if he held security clearance eligibility before 2013. (AE 4-5.)

In February 2016, Applicant accepted an offer of employment from Company A. He tendered his resignation to Company B on February 18, 2016. Following internal protocol, the facility security officer (FSO) informed Company B's counterintelligence group that Applicant was going to work for a competitor, Company A, in a position in the same technology area. After determining that Applicant had critical intellectual property knowledge and access, the counterintelligence group performed a due-diligence review to identify the movement of any Company B data to external media or non-Company B email addresses. The review revealed that Applicant transferred over 93,000 Company B files, including 25,000 related to a project that Applicant worked on between 1994 and 2013, to two personal storage devices. While it is unclear when Applicant started transferring these files, Company B noted that 48,600 of the files were transferred between January and February 2016. The downloaded information included Company B proprietary information, both technical and business-related, foreign military information, and sensitive, unclassified DOD program information. Company B determined that use or disclosure of the information by Applicant could cause potential loss of competitive advantage to Company B and could cause potential damage to U.S. interests. (GE 5-6, 10-11.)

On February 19, 2016, a Company B counterintelligence investigator interviewed Applicant. The FSO and a human resources representative were also present for the interview. At the beginning of the interview, the investigator had Applicant review Company B's policy regarding the ownership and protection of proprietary information, as well as Company's B policy on internal investigations. According to the investigative report, Applicant signed an acknowledgement certifying that he did not retain any Company B proprietary information. During the interview, Applicant repeatedly denied transferring Company B data to personal devices, even when asked about the specific devices he used. He admitted transferring the files only after the investigator confronted him with direct evidence. He explained that the downloaded files represented his life's work and that he wanted to have it available to him in his role at Company A for personal reference only. (GE 7-10.)

At Company B's direction, Applicant retrieved the two storage devices from his home and surrendered them for examination. He was then placed on administrative leave pending a forensic review of the devices and a decision from management on how to handle the situation. A forensic review of the devices revealed that Applicant transferred over 200,000 files, the majority of which belonged to Company B, including over 25,000 related to a specific program. The forensic review also seemed to suggest Applicant was transferring data to personal devices as early as 2012. (GE 7-10.)

The investigation confirmed that Applicant transferred Company B proprietary and sensitive data to personal devices in violation of the company's IT policy regarding the introduction and storage of Company B data on unauthorized devices. On February 24, 2016, Company B issued Applicant an order requiring his immediate resignation in lieu of termination. Company B also sent a letter to Company A informing them of Applicant's actions and to place Company A on notice not to make use of any Company B proprietary information provided to them by Applicant. Company B referred the matter to the FBI for further investigation. The FBI referred the case to the U.S. Attorney's Office, seeking a warrant to search Applicant's home for additional materials and for prosecution under 18 U.S.C. ¶ 1832, "Theft of Trade Secrets." The U.S. Attorney's office declined to pursue the case. (GE 10-11.)

Applicant admits he lied during the Company B interview, but denies he downloaded the files for any nefarious purposes. In his response to the FORM, Applicant explained that he began blindly backing up all of his professional files in 2000 to preserve the work he generated for his personal use. He lied during the Company B interview because he was scared. Applicant considers himself an honest person who exhibited extremely poor judgment in violating Company B's policies. He vows not to violate his employer's rules in the future. (GE 3-4; AE A.)

Policies

When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the adjudicative guidelines. In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially

disqualifying conditions and mitigating conditions, which are to be used in evaluating an applicant's eligibility for access to classified information.

These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, administrative judges apply the guidelines in conjunction with the factors listed in the adjudicative process. The administrative judge's overarching adjudicative goal is a fair, impartial, and commonsense decision. According to AG ¶ 2(a), the entire process is a conscientious scrutiny of a number of variables known as the "whole-person concept." The administrative judge must consider all available, reliable information about the person, past and present, favorable and unfavorable, in making a decision.

The protection of the national security is the paramount consideration. AG ¶ 2(b) requires that "[a]ny doubt concerning personnel being considered for national security eligibility will be resolved in favor of the national security." In reaching this decision, I have drawn only those conclusions that are reasonable, logical, and based on the evidence contained in the record.

Under Directive ¶ E3.1.14, the Government must present evidence to establish controverted facts alleged in the SOR. Under Directive ¶ E3.1.15, the applicant is responsible for presenting "witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by the applicant or proven by Department Counsel." The applicant has the ultimate burden of persuasion to obtain a favorable security decision.

A person who seeks access to classified information enters into a fiduciary relationship with the Government predicated upon trust and confidence. This relationship transcends normal duty hours and endures throughout off-duty hours. The Government reposes a high degree of trust and confidence in individuals to whom it grants access to classified information. Decisions include, by necessity, consideration of the possible risk the applicant may deliberately or inadvertently fail to safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation of potential, rather than actual, risk of compromise of classified information.

Analysis

The record establishes that Applicant engaged in disqualifying conduct under the use of information technology and personal conduct guidelines. Applicant engaged in conduct that raises concerns about his ability to handle and protect sensitive and classified information and his ability to follow rules and regulations. His misconduct also highlights concerns about his judgment, trustworthiness and reliability. (See AG ¶¶ 39 and 15).

Applicant violated his employer's IT policy relating to the introduction and storage of Company B data on unauthorized devices. (AG ¶ 40(e)). An internal investigation revealed that from as early as 2012 to February 2016, Applicant transferred over 200,000 files containing Company B's proprietary or other protected information onto

two unauthorized personal storage devices. (AG ¶¶ 40(d)). This conduct is particularly egregious given that Applicant transferred approximately 48,600 files, the month before he tendered his resignation at Company B to begin employment with Company A, a known competitor. In addition to improperly transferring files to personal storage devices, Applicant deliberately provided false statements to the Company B investigator until after being confronted with evidence of his misconduct. (AG ¶ 16(b)).

None of the use of IT systems or personal conduct mitigating conditions apply. Applicant describes himself as an honest person who exhibited bad judgment. The record does not support this characterization. Applicant claims that his motive was benign, to preserve what he considered his "life's work," but the vast number of files he downloaded before tendering his resignation to work for a competitor casts doubt on that motive. Applicant's disregard of Company B's IT policy was not a minor, isolated exercise of poor judgment. He engaged in intentional misconduct to preserve his self-interest at the potential detriment to his employer and U.S. interests. Furthermore, Applicant failed to provide truthful and candid answers during the Company B investigation. Applicant's statements regarding his actions on his August 2016 security clearance application were in line with his conduct during the Company B internal investigation. Applicant offered enough information to convey an adverse employment action. However, the disclosure did not relate the actual misconduct and minimized the nature and extent of it.

Based on the record, doubts remain about Applicant's reliability, trustworthiness, good judgment, and ability to protect classified or sensitive information. In reaching this conclusion, I have also considered the whole-person factors enumerated in AG ¶ 2(d). Applicant has worked for federal contracting companies for over 30 years. He undoubtedly understood the importance of handling and safeguarding proprietary, sensitive, and classified information and chose to disregard his obligation to do so. The purpose of the security clearance adjudication is to make "an examination of a sufficient period of a person's life to make an affirmative determination that the person is an acceptable security risk." (AG ¶ 2(d)). Applicant violated his employer's policies and potentially risked U.S. interests to advance his self-interests. Furthermore, he has demonstrated that he cannot be relied upon to admit, let alone self-report adverse information. Applicant's conduct creates a security risk that must be resolved in favor of the government.

Formal Findings

The formal findings on the SOR allegations are:

Paragraph 1, Guideline M:	Against Applicant
Subparagraph 1.a:	Against Applicant
Paragraph 2, Guideline E:	Against Applicant
Subparagraph 2.a:	Against Applicant

Conclusion

It is not clearly consistent with the national interest to grant Applicant access to classified information. Eligibility denied.

Nichole L. Noel
Administrative Judge