DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEA

In the matter of:	)	
	)	
	)	ISCR Case No. 19-02995
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Kelly Folks, Esq., Department Counsel
For Applicant: *Pro se*

12/06/2021

Decision

Curry, Marc E., Administrative Judge:

Applicant downloaded multiple files, including company proprietary information, from his company drive to his personal external hard drive in violation of company policy. This generated a security concern that he failed to mitigate. Clearance is denied.

Statement of the Case

On December 13, 2019, the Department of Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) to him, detailing the security concerns under Guidelines K and M, explaining why it was unable to find it clearly consistent with the national interest to grant security clearance eligibility. The DOD CAF took the action under Executive Order (EO) 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; and DOD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive) and the National Security Adjudicative Guidelines (AG), effective June 8, 2017. On January 27, 2020, Applicant admitted the allegation and requested a hearing. On June 2, 2021, the case was assigned to me, and on July 23, 2021, a notice of video teleconference hearing was issued, scheduling the case for August 10, 2021.

The hearing was held as scheduled. I received six government exhibits, marked and incorporated into the record as Government Exhibits (GE) 1 to 6, and I received Applicant's testimony. At the end of the hearing, I left the record open at Applicant's request to allow him the opportunity to submit additional exhibits. Within the time allotted, he submitted eight exhibits that I incorporated into the record as Applicant Exhibit (AE) A to AE H. The transcript (Tr.) was received on August 19, 2021.

Findings of Fact

Applicant is a 60-year-old married man with two adult children. He has a college degree in the field of computer science, a master's degree in management, and a master's degree of business administration. (Tr. 20) Applicant has been working in the defense contracting industry for nearly 40 years. For much of that time, he has worked in advanced logistics and hardware engineering. (Tr. 25) Applicant joined his current company in 2017, after having worked for his previous employer since 1984. (Tr. 20) He has held a security clearance for his entire career. (Tr. 14, 31)

In April 2017, approximately four months before Applicant began his current job, he downloaded 9,000 files from the company drive of his then-employer to a personal hard drive and a personal removable media drive. (Answer at 1; 43) Some of the downloaded files contained sensitive and proprietary information, including templates, proprietary coursework, and competition-sensitive operational data and cost volume information about a proposal that his company was working on. (Tr. 26, 49; 2 at 6; GE 4 at 3; GE 6 at 10, 17**)** Company policy prohibited downloading of proprietary information onto personally owned devices. (GE 4 at 3)

Applicant contends that he had no intention to steal any proprietary information, and that he was unaware that any of the information that he transferred to his personal media devices was proprietary. (Tr. 11, 37) Rather, his intent was to back up his "samples" folder of all of the different methods that he used over the years to perform his job. Applicant's "samples" folder contained a collection of all of the lessons that he learned during his career, in addition to various code that he had written over the years. (Tr. 12, 21-22) Applicant considered it his personal intellectual property. (Tr. 66) Moreover, he contends that it was common practice to store company information on personal thumb drives before the policy was changed in 2014. (Tr. 34) When Applicant first began backing up what he thought to be non-proprietary information, a pop-up information technology warning banner appeared on his computer screen, informing him that he should not connect a personal device to a company asset. (Tr. 43; Answer at 3; GE 2 at 5; Tr. 35) Nevertheless, he proceeded with the information transfer. (Answer at 3)

The most files that Applicant ever downloaded in his career with his employer before the download in April 2017, was five. (GE 4 at 2) The size of Applicant's download and the amount of time that it engaged his work computer to complete it prompted a company investigation in May 2017. (GE 6 at 1) The investigation was spearheaded by the director of capture management and the lead investigator of the division where Applicant worked.

Applicant's company issues its employees external hard drives for data backups. (GE 6 at 27; Tr. 40) When the investigator asked Applicant during his interview why he used a personal device for his information device rather than the device that his company issued, Applicant explained that he needed a second backup in the event that he lost the primary backup while traveling or working from home. (GE 6 at 27) This explanation made no sense to either the director of capture management or the investigator. (GE 6 at 27) At the conclusion of the investigation in August 2017, the capture management manager was still reviewing the contents of the downloaded files and continuing to discover sensitive proprietary information. (GE 4 at 3

By the time the investigation was completed, Applicant had retired, left the company, and begun working for his current employer. (GE 1 at 11) The investigator had retrieved the external drive from Applicant and wiped it shortly after initiating the investigation. (Tr. 58) The job Applicant took after retiring from his previous employer was director-level, a position that paid substantially more money than his previous position. (GE 2 at 7) Applicant informed his current supervisor of the episode. (Tr. 28)

Applicant characterizes his conduct as a good-faith mistake in judgment when he assumed that all of the information was his personal intellectual property rather than his employer's intellectual property. Moreover, he contends that he had no intention of damaging his company financially by sharing its intellectual property with competitors because "that's where [his] pension is coming from." (Tr. 29)

Applicant is highly respected on the job and in his community. He is active in his church, and spends hours working with youth in the community, coaching basketball and leading a Cub Scout troop. (AE C, D) According to a current coworker, his compliance with regulations is exceptional. (AE A) Another coworker characterized him as "a person of extreme integrity." (AE E) A coworker from his previous job characterized him as "honest, conscientious, dedicated, and helpful." (AE B) According to Applicant's wife, he is an extremely meticulous individual who organizes playbooks for the youth teams he coaches and annotates the repair manuals for their home appliances. (AE D)

Policies

The U.S. Supreme Court has recognized the substantial discretion the Executive Branch has in regulating access to information pertaining to national security, emphasizing that "no one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988). 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 required to be considered 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, these guidelines are applied in conjunction with the factors listed in the adjudicative process. The administrative judge's overall adjudicative goal is a fair, impartial, and commonsense decision. According to AG ¶ 2(c), 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 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 that the applicant may deliberately or inadvertently fail to safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation about potential, rather than actual, risk of compromise of classified information. Section 7 of Executive Order 10865 provides that decisions shall be "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." *See also* EO 12968, Section 3.1(b) (listing multiple prerequisites for access to classified or sensitive information).

Under the whole-person concept, the administrative judge must consider the totality of an applicant's conduct and all relevant circumstances in light of the nine adjudicative process factors in AG ¶ 2(d).[1]

Analysis

Guideline K: Handling Protected Information

Under this guideline, "deliberate or negligent failure to comply with rules and regulations for handling protected information --- which includes classified and other

[1] The factors under AG ¶ 2(d) are as follows:

> (1) the nature, extent, and seriousness of the conduct; (2) the circumstances surrounding the conduct, to include knowledgeable participation; (3) the frequency and recency of the conduct; (4) the individual's age and maturity at the time of the conduct; (5) the extent to which participation is voluntary; (6) the presence or absence of rehabilitation and other permanent behavioral changes; (7) the motivation for the conduct; (8) the potential for pressure, coercion, exploitation, or duress; and (9) the likelihood of continuation or recurrence.

sensitive government information, and proprietary information --- raises doubt about an individual's trustworthiness, judgment, reliability, or willingness and ability to safeguard such information, and is a serious security concern." (AG ¶ 33) Applicant's transfer of 9,000 files from his work network to a personal external drive, in violation of company regulation, triggers the application of AG ¶ 34(e), "loading drafting, editing, modifying, storing, transmitting, or otherwise handling protected information, including images, on any unauthorized equipment or medium."

Applicant has enjoyed a successful career, and is highly respected in the community. The episode that forms the basis of the SOR was the only failure of handling protected information in Applicant's 37-year career, and more than four years have elapsed since its occurrence. Conversely, his security misuse of information technology was egregious, as he downloaded sensitive information in violation of company regulation, continuing to do so despite a warning banner that appeared on his computer screen informing him that his action was inappropriate. Moreover, both the investigator and the director of capture management questioned the credibility of his explanation as to why he did not simply back up the information that he thought was personal on the external drives that their employers issued to employees. Under these circumstances, although AG ¶ 35 (a), "so much time has elapsed since the behavior, or it has happened so infrequently, or under such unusual circumstances, that it is unlikely to recur and does not case doubt on the individual's current reliability, trustworthiness, or good judgment," is partially applicable, insofar as the incident was isolated, and several years have elapsed since it occurred, the nature and seriousness of the incident continues to cast doubt on Applicant's security-clearance worthiness. I conclude Applicant has failed to mitigate the security concern regarding handling protected information.

Guideline M: Use of Information Technology

Under this guideline, "failure to comply with rules, procedures, guidelines, or regulations pertaining to information technology systems may raise security concerns about an individual's reliability and trustworthiness, calling into question the willingness or ability to property protect sensitive systems, networks, and information." (AG ¶ 39) Applicant's conduct triggers the application of AG ¶ 40(d), "downloading, storing, or transmitting classified, sensitive, proprietary, or other protected information on or to any unauthorized information technology system," and AG ¶ 40(f), "introduction, removal, or duplication of hardware, firmware, software, or media to or from any information technology system when prohibited by rules, procedures, guidelines, or regulations or when otherwise not authorized." Applicant's conduct is disqualifying under this guideline for the same reasons that it is disqualifying under the handling of protected guidelines, as discussed above.

Whole-Person Concept

Applicant's career has been impressive. For the past four years, he has been working in a more lucrative position with greater responsibilities than the job that he held with his previous employer. This positive attributes, however, are outweighed by the nature and seriousness of Applicant's misuse of information technology.

Formal Findings

Formal findings for or against Applicant on the allegations set forth in the SOR, as required by section E3.1.25 of Enclosure 3 of the Directive, are:

Paragraph 1, Guideline K:	AGAINST APPLICANT
Subparagraphs 1.a:	Against Applicant
Paragraph 2, Guideline M:	AGAINST Applicant
Subparagraph 2.a:	Against Applicant

Conclusion

In light of all of the circumstances presented by the record in this case, it is not clearly consistent with the interests of national security to grant Applicant eligibility for a security clearance. Eligibility for access to classified information is denied.

_____
Marc E. Curry
Administrative Judge