DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 19-02040
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Aubrey M. De Angelis, Esq., Department Counsel
For Applicant: Frederic G. Nicola, Esq.

12/14/2021

_____

Decision

_____

LOUGHRAN, Edward W., Administrative Judge:

Applicant did not mitigate the personal conduct and handling protected information security concerns. Eligibility for access to classified information is denied.

Statement of the Case

On October 4, 2019, the Department of Defense (DOD) issued a Statement of Reasons (SOR) to Applicant detailing security concerns under Guidelines E (personal conduct) and K (handling protected information). Applicant responded to the SOR on November 8, 2019, and requested a hearing before an administrative judge. The case was assigned to three other administrative judges before being reassigned to me on July 7, 2021.

The hearing was convened as scheduled on August 5, 2021. Government Exhibits (GE) 1 through 3 were admitted in evidence without objection. Applicant testified and submitted Applicant's Exhibits A, which was admitted in evidence without objection.

Findings of Fact

Applicant is a 49-year-old employee of a defense contractor (Company B). She has worked for her current employer since April 2017. She seeks to retain a security clearance, which she has held since about 2003. She earned a bachelor's degree in 2006. She is married for the third time after two divorces. She has an adult child. (Transcript (Tr.) at 15-17,44; GE 1, 3)

Applicant worked as a cybersecurity specialist for a defense contractor (Company A) from 2009 until she was terminated in March 2017 after allegations of poor performance, timecard fraud, and copying proprietary information onto a thumb drive. Applicant's section failed an inspection in November 2016. Her title and salary remained the same after the inspection, but she no longer supervised employees. She went to human resources (HR) in November 2016 with a complaint that she was blamed for the failure. On January 14, 2017, she again reported to HR what she viewed as unethical practices by the company's leadership. (Tr. at 17, 33-34; GE 1-3)

In about November or December 2016, Applicant sought employment with Company B. On February 7, 2017, Company B sent her a welcome-to-the company email with information about her pre-employment actions to complete, including a drug test. Applicant's supervisors at Company A had difficulty locating her in January and February 2017. On February 8, 2017, Applicant was given a verbal warning regarding her absences and her inability to be contacted by fellow employees. On February 8, 2017, Applicant downloaded about 3,000 files from her Company A computer and server onto an unencrypted thumb drive. The files included 32 personal files, and the rest were Company A's files. (Tr. at 27, 33-36, 51; Applicant's response to SOR; GE 2)

On February 9, 2017, Applicant's management chain requested the company to conduct an investigation into suspected timecard fraud. On February 14, 2017, Applicant was interviewed by the investigators about her hours and about the files on the thumb drive. (Tr. at 27; GE 2)

Applicant testified that she gave her employer two weeks' notice on February 14, 2017, before the investigation was initiated. There is nothing in Company A's report of the investigation to substantiate that assertion. Company A was aware from reviewing Applicant's computer that Company B had requested that she undergo a drug test. She was asked if she had a job offer from Company B. She stated that she accepted the job offer, but a start date was yet to be determined until all contingencies were met. Applicant was placed on paid suspension until the investigation was complete. She was terminated by Company A on March 17, 2017. Applicant asserted that Company A's actions against her were because of her whistleblower report to HR. (Tr. at 22-23; Applicant's response to SOR; GE 2)

Applicant stated that she was not terminated from Company A because she voluntarily resigned to take the job with Company B before she was terminated. I note that she reported on her Questionnaire for National Security Positions (SF 86) in November 2017 that she was "Fired," and her attorney noted in her response to a

proposed debarment that Applicant was "terminated" in retaliation after she reported unethical conduct to HR and she gave notice of her intent to resign. Applicant was successful in the debarment action. (Tr. at 22-23, 40-44; Applicant's response to SOR; GE 1) For the purpose of this decision, it makes little difference whether Applicant was terminated or resigned before she could be terminated. The underlying conduct is the issue here.

Applicant denied the allegation of timecard fraud. Company A investigators checked Applicant's timecards against the records of when she swiped into her work facility, and determined that over a six-month period, there was a discrepancy of 294 hours. Applicant asserted, and her supervisor confirmed, that her supervisor permitted Applicant to unofficially work from home. Additionally, the investigators checked Applicant's primary facility, but the company had another facility a few miles away. The records would not show all the time she spent at that facility and traveling back and forth between the facilities. Finally, Applicant's supervisor suspected that Applicant was not working all of the hours that she reported on her timecards, but with the approval of the supervisor above her, they chose not to question Applicant about her hours, and just approved Applicant's timecards. (Applicant's response to SOR; GE 2, 3)

During her interview by Company A investigators on February 14, 2017, Applicant admitted that she downloaded the files. She stated that she was backing up her personal files, and found it easier to copy her entire directory and go to a meeting while the files were being copied. She stated that she planned to delete the Company A files from the thumb drive, but had not had the opportunity to do so. (Tr. at 27; GE 2)

The investigation determined that it took 68 minutes to download the more than 3,000 files onto the thumb drive. It would have taken less than two minutes to download Applicant's personal files. The investigation concluded that Applicant is an experienced cybersecurity professional who knew it was inappropriate to use an unapproved and unencrypted thumb drive to download Company A proprietary information. (GE 2)

Applicant testified that she "inadvertently" and "purely by accident" transferred the Company A proprietary files along with her personal files to the thumb drive, and that it was never her intention to download or keep the files. She stated that it was a simple swipe to download everything, and that she did not notice that it took more than an hour to download the files because she went to a meeting. Applicant's assertion that she "inadvertently" downloaded the files is inconsistent with her statement to Company A investigators in February 2017 that she found it easier to copy her entire directory. She indicated that she knew that plugging in the thumb drive would prompt a report to the security office; she self-reported the incident to the security office; and she returned the thumb drive the same day that the files were downloaded. That assertion is inconsistent with the report of the investigation that showed the files were downloaded on February 8, 2017, and Applicant provided the thumb drive on February 14, 2017, when she was interviewed. She later testified that she went to security on February 8, 2017, who told her that copying her own personal files was not against their rules and procedures. (Tr. at 27-30, 37-40, 44-45, 51-54; GE 2)

Applicant submitted a Questionnaire for National Security Positions (SF 86) in November 2017. She reported the timecard issues with Company A, but she did not report that she downloaded Company A's proprietary files without the company's authorization. Even if the downloading was inadvertent, she should have reported the information under the Use of Information Technology Systems question that asked: "**In the last seven (7) years** have you introduced, removed, or used hardware, software, or media in connection with any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines, or regulations or attempted any of the above?"[1] (GE 1)

During her March 2019 interview for her background investigation, Applicant discussed the timecard allegations. She also indicated that she downloaded personal files onto a thumb drive. There is no indication in the report of the interview that she also downloaded Company A's files. In her response to the SOR allegation that she downloaded about 3,000 Company A files onto a thumb drive, she wrote:

> **I partially admit.** While working at [Company A] for approximately 8 years I worked on numerous computer systems; one work station which could be considered my personal work computer which housed unclassified information and numerous other work stations which did contain classified information. After I accepted my new job at [Company B] I transferred what I had accumulated on my "personal work computer" to a thumbdrive. Things included were tax returns, leases, receipts and various other personal items; I admit I should not have had these items on my computer. Nonetheless when leaving [Company A] I transferred all my files. I would note that nothing on my computer was classified at all. I knew this when I took this action.
>
> I was contacted shortly after that [Company A's system] put out a notification of this transfer. Once notified I immediately returned the thumbdrive with all files. I did not download any file to any computer including all of my personal documents.

I did not find Applicant credible. After considering all of the evidence, I find that she intentionally downloaded Company A proprietary information, and she has been less than forthcoming about her conduct up to and during her hearing.

Applicant submitted documents and letters attesting to her character and excellent job performance, both at Company A and Company B. She is praised for her work ethic, patience, mentoring skills, positive attitude, technical proficiency, leadership, stability, discretion, dependability, professionalism, trustworthiness, and reliability. (Applicant's response to SOR; AE A)

[1] Any matter that was not alleged in the SOR will not be used for disqualification purposes. It may be considered in assessing Applicant's credibility, in the application of mitigating conditions, and when conducting the whole-person analysis.

Policies

This case is adjudicated under Executive Order (EO) 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; DOD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the adjudicative guidelines (AG), which became effective on June 8, 2017.

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(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."

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.

Section 7 of EO 10865 provides that adverse 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).

Analysis

Guideline K, Handling Protected Information

The security concern for handling protected information is set out in AG ¶ 33:

> Deliberate or negligent failure to comply with rules and regulations for handling protected information-which includes classified and other 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 ¶ 34 describes conditions that could raise a security concern and may be disqualifying. The following are potentially applicable:

> (b) collecting or storing protected information in any unauthorized location; and
>
> (g) any failure to comply with rules for the protection of classified or sensitive information.

Applicant used an unapproved and unencrypted thumb drive to download Company A proprietary information. The above disqualifying conditions are established.

Conditions that could mitigate handling protected information security concerns are provided under AG ¶ 35. The following are potentially applicable:

> (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 cast doubt on the individual's current reliability, trustworthiness, or good judgment;
>
> (b) the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities;
>
> (c) the security violations were due to improper or inadequate training or unclear instructions; and
>
> (d) the violation was inadvertent, it was promptly reported, there is no evidence of compromise, and it does not suggest a pattern.

There is only one Guideline K allegation and that occurred almost five years ago. Had Applicant accepted full responsibility for her conduct, she might have mitigated the conduct. However, as discussed above, she has been less than forthcoming about her conduct up to and during her hearing. I am unable to find that the conduct is unlikely to

recur. It continues to cast doubt on her current reliability, trustworthiness, and good judgment. The above mitigating conditions are not applicable.

Guideline E, Personal Conduct

The security concern for personal conduct is set out in AG ¶ 15, as follows:

> Conduct involving questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations can raise questions about an individual's reliability, trustworthiness and ability to protect classified information. Of special interest is any failure to provide truthful and candid answers during the security clearance process or any other failure to cooperate with the security clearance process.

AG ¶ 16 describes conditions that could raise a security concern and may be disqualifying. The following disqualifying conditions are potentially applicable:

> (c) credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any other single guideline, but which, when considered as a whole, supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the individual may not properly safeguard classified or sensitive information;
>
> (d) credible adverse information that is not explicitly covered under any other guideline and may not be sufficient by itself for an adverse determination, but which, when combined with all available information, supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the individual may not properly safeguard classified or sensitive information. This includes, but is not limited to, consideration of:
>
> > (1) untrustworthy or unreliable behavior to include breach of client confidentiality, release of proprietary information, unauthorized release of sensitive corporate or government protected information;
> >
> > (3) a pattern of dishonesty or rule violations;
> >
> > (4) evidence of significant misuse of Government or other employer's time or resources; and
>
> (e) personal conduct, or concealment of information about one's conduct, that creates a vulnerability to exploitation, manipulation, or duress by a foreign intelligence entity or other individual or group. Such conduct includes:

(1) engaging in activities which, if known, could affect the person's personal, professional, or community standing.

Applicant's downloading of Company A proprietary information is cross-alleged under Guideline E. That conduct reflects questionable judgment and an unwillingness to comply with rules and regulations. The conduct also created vulnerability to exploitation, manipulation, and duress. AG ¶ 16(e) is applicable. AG ¶ 16(c) is not perfectly applicable because that conduct is sufficient for an adverse determination under the handling protected information and use of information technology guidelines. However, the general concerns about questionable judgment and an unwillingness to comply with rules and regulations contained in AG ¶¶ 15 and 16(c) are established.

The timecard fraud allegation is less clear. There is a discrepancy between Applicant's timecards and the records of when she swiped into her work facility. However, that does not account for when Applicant's supervisor permitted her to unofficially work from home and the time Applicant spent at and traveling to and from the second facility. Finally, Applicant's supervisor suspected that Applicant was not working all of the hours that she reported on her timecards, but with the approval of a higher-level supervisor, they chose not to question Applicant about her hours, and just approved Applicant's timecards. I am not convinced that Applicant committed the extensive timecard fraud reported in the investigation. Any discrepancy between the hours Applicant actually worked and what she reported on her timecards is mitigated. SOR ¶ 1.a is concluded for Applicant.

AG ¶ 17 provides conditions that could mitigate security concerns. The following are potentially applicable:

(c) the offense is so minor, or so much time has passed, or the behavior is so infrequent, or it happened under such unique circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment;

(d) the individual has acknowledged the behavior and obtained counseling to change the behavior or taken other positive steps to alleviate the stressors, circumstances, or factors that contributed to untrustworthy, unreliable, or other inappropriate behavior, and such behavior is unlikely to recur; and

(e) the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress.

The handling protected information analysis applies equally here. Personal conduct security concerns are not mitigated.

Whole-Person Concept

Under the whole-person concept, the administrative judge must evaluate an applicant's eligibility for a security clearance by considering the totality of the applicant's conduct and all relevant circumstances. The administrative judge should consider the nine adjudicative process factors listed at AG ¶ 2(d):

> (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.

Under AG ¶ 2(c), the ultimate determination of whether to grant eligibility for a security clearance must be an overall commonsense judgment based upon careful consideration of the guidelines and the whole-person concept. I have incorporated my comments under Guidelines E and K in my whole-person analysis. I also considered Applicant's character evidence, but the favorable information is insufficient to overcome her problematic conduct and failure to accept responsibility for that conduct.

Overall, the record evidence leaves me with questions and doubts about Applicant's eligibility and suitability for a security clearance. I conclude Applicant did not mitigate the personal conduct and handling protected information security concerns.

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 E:	Against Applicant
Subparagraph 1.a:	For Applicant
Subparagraph 1.b:	Against Applicant
Paragraph 2, Guideline K:	Against Applicant
Subparagraph 2.a:	Against Applicant

Conclusion

It is not clearly consistent with the national interest to continue Applicant's eligibility for a security clearance. Eligibility for access to classified information is denied.

_____
Edward W. Loughran
Administrative Judge