DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 17-01817
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Daniel Crowley, Esq., Department Counsel
For Applicant: *Pro se*

02/26/2020

_____

Decision

_____

COACHER, Robert E., Administrative Judge:

Applicant failed to mitigate the security concerns under Guideline E, personal conduct, Guideline J, criminal conduct, and Guideline M, use of information technology. Applicant's eligibility for a security clearance is denied.

History of the Case

On November 14, 2017, the Department of Defense (DOD) issued Applicant a Statement of Reasons (SOR) detailing security concerns under Guidelines E, J, and M. The DOD acted 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) implemented by the DOD on June 8, 2017. (The SOR in this case was styled as an automated data processing

(ADP) trustworthiness determination, however, I have determined that Applicant was being sponsored by her employer for a security clearance (*See* HE III). This case will be treated as a security clearance determination.

Applicant answered the SOR on December 5, 2017, and requested a hearing. (This case is dated because Applicant lost her original employer sponsorship in 2017 and the processing of her case ceased at that time. Upon recently receiving new sponsorship, Applicant's case processing was resumed.) The case was assigned to me on November 26, 2019. The Defense Office of Hearings and Appeals (DOHA) issued a notice of hearing on December 9, 2019, and the hearing was held as scheduled on January 9, 2020. The Government offered exhibits (GE) 1-8, which were admitted into evidence without objection. The Government's discovery letter to Applicant was marked as hearing exhibit (HE) I and the Government's exhibit list was marked as HE II. Applicant testified and presented the testimony of one witness. She offered exhibits (AE) A-H, which were all admitted without objection. DOHA received the hearing transcript (Tr.) on January 17, 2020.

Findings of Fact

Applicant admitted SOR ¶¶ 1.a, 2.a, and 3.a-3.c, with explanations, and denied SOR ¶¶ 1.b-1.c. The admissions are adopted as findings of fact. After a thorough and careful review of the pleadings and exhibits submitted, I make the following additional findings of fact.

Applicant is 49 years old. She has never married and has one child. She is seeking a position requiring a security clearance. She previously held a security clearance before it was revoked by another government agency (AGA) in 2013. She currently works as an information technology (IT) systems engineer. She has worked for her current employer (her clearance sponsor) since June 2018. She holds a bachelor's degree. She also owns a fitness business. (Tr. 11-8; 46; GE 5-8)

The SOR alleged, under Guideline E, that Applicant committed employee theft between 1989 and 1990 by stealing approximately 25 pieces of clothing (SOR ¶ 1.a). It also alleged that between 2000 and 2005, while employed by employer-1 (E1), and between 2005 and 2007, while employed by employer-2 (E2), Applicant stole numerous computer hardware items, including computer towers, monitors, keyboards, mouse sets, speakers, laptop computers, memory sticks, a hard drive, and a digital scanner (SOR ¶¶ 1.b-1.c). The employee theft of clothing was also alleged as criminal activity (SOR ¶ 2.a). Under Guideline M, the SOR alleged that Applicant engaged in illegal downloading of movies from 1993-2008; music from 2008-2011; and computer software, games, and emulators (SOR ¶¶ 3.a-3.c).

In December 2011, Applicant's employer sponsored her for access to AGA's sensitive compartmented information (SCI). Applicant held a top secret clearance at that

time. A corresponding background investigation ensued and Applicant was interviewed and required to take a polygraph examination. In March 2012, during her interview, Applicant admitted that in approximately 1990, she used stolen credit cards to purchase clothing items. The credit cards were from a customer who reported her purse stolen from the store where Applicant worked. A police investigation revealed Applicant and her friend as the crime perpetrators. She was charged with felony theft, but the charges were reduced to misdemeanors. She paid restitution and served a work-release sentence. (Tr. 48; GE 2-5)

Also during the March 2012 interview, Applicant admitted that while working for two different employers (one was a successor contractor to the other) from 2000 to 2007 she took, without permission or authorization, numerous computer items, including multiple computer towers, monitors, keyboards, mouse sets, speakers, and memory sticks. She also took at least three laptop computers. She used these herself at home and gave several away to family members, her friends, and even her church. The value of the items was in excess of several thousands of dollars. She explained to the interviewer that she took the items because she could not afford to buy similar items at the time and the company was overstocked with these surplus items. She was told by a government employee that the items were to be strictly accounted for, but he also insinuated that he did not care if she took things. She knew what she was doing was wrong and she stopped. In her SOR answer and during her testimony, Applicant backed away from total acceptance of responsibility for her actions and claimed she had verbal authority from a supervisor to take the items. She also claimed that there was a culture of permissiveness when it came to computer accountability at these companies during that time. Her SOR responses on this issue and her testimony were not credible. (Tr. 47; GE 5-6, 8)

Applicant further related, during her March 2012 interview, that she engaged in illegally downloading of music, movies, software, games, and emulators from approximately 1993 to 2011. She estimated that she downloaded over 10,000 songs valued at over $10,000 and over hundreds of movies valued at over $5,000. She engaged in this activity using her personal computer equipment and other times using her employer's computers and peripherals. She also illegally downloaded software, game programs, and emulators valued at between $400 and $1,000. Between 2002 and 2007, she also downloaded music and movies from a government server without authorization. In her hearing testimony, Applicant claimed that the permissive culture at the government agency allowed the downloading from the government server for personal use. (Tr. 47; GE 5, 6)

Applicant's actions described above were fully investigated by AGA and she was denied SCI access in December 2012. Applicant appealed that decision in February 2013, and the denial decision was sustained in March 2013. (GE 5-7)

Applicant's former supervisor from 2006 to 2007 testified that he had no personal knowledge of Applicant taking company property during that timeframe. He commented that there was a lack of accountability standards at the company when he took over his position in 2006. Even though he has not worked with Applicant since that time, he has stayed in contact with her and is not aware of any other bad acts on her part. He believes that she learned from this incident and has grown because of it. (Tr. 37, 39-41, 43-44)

Applicant also presented written letters of thanks from a former employer in 2016, and a certificate of excellence from her employer in 2008. She presented a letter from her supervisor in 2018 who fully described her talents and skills within their organization. He further described Applicant as a reliable and trustworthy employee. Additionally, Applicant presented documentation showing her active community involvement by restoring a local residence for cancer patients and her participation in a local community workgroup. She is described as an intelligent, caring, and excellent team player. Applicant testified that, other than traffic tickets, she has not had any further involvement with law enforcement. (Tr. 51; AE A-C, E, H)

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 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, these guidelines are applied 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 careful weighing 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, an "applicant is

responsible for presenting witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by applicant or proven by Department Counsel, and 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 an 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 EO 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).

Analysis

Guideline E, Personal Conduct

AG ¶ 15 expresses the personal conduct security concern:

> 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 or sensitive information. Of special interest is any failure to cooperate or provide truthful and candid answers during national security investigative or adjudicative processes. . . .

AG ¶ 16 describes conditions that could raise a security concern and may be disqualifying in this case. The following disqualifying condition is 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.

The record evidence is sufficient for an adverse determination under the criminal conduct guideline, nevertheless, as a whole, Applicant's actions put into issue her judgment, trustworthiness and overall personal conduct, as expressed in the general security concern in AG ¶15 and the specific concern expressed in AG ¶ 16(c). Applicant's criminal incidents in about 1990 and between 2000 and 2007 raise questions about her reliability, trustworthiness, and judgment.

I have also considered all of the mitigating conditions for personal conduct under AG ¶ 17 and considered the following relevant:

> (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; and
>
> (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.

Appellant's crimes of theft and fraud back in 1990, when she was 20 years old, are remote and unique, qualifying for some mitigating consideration under AG ¶ 17(c). However, full mitigation is not appropriate given Applicant's continuing untrustworthy behavior years later by taking computer equipment without proper authority and illegally downloading computer programs, music, and movies to include doing so from a government server without authorization. Her actions cast doubt on her reliability, trustworthiness, and judgment. AG ¶ 17(c) does not fully apply. While Applicant initially accepted responsibility for her actions, she more recently backed away from that responsibility, seeking to lay blame on a permissive work culture that allowed her to take property that was not hers in the form of computer hardware, software, and other computer media. Applicant receives some credit under AG ¶ 17(c), but, AG ¶ 17(d) does not apply.

Guideline J, Criminal Conduct

The security concern relating to the guideline for criminal conduct is set out in AG ¶ 30:

> Criminal activity creates doubt about a person's judgment, reliability, and trustworthiness. By its very nature, it calls into question a person's ability or willingness to comply with laws, rules and regulations.

AG ¶ 31 describes conditions that could raise a security concern and may be disqualifying in this case. The following is potentially applicable:

> (b) evidence (including, but not limited to, a credible allegation, an admission, and matters of official record) of criminal conduct, regardless of whether the person was formally charged, formally prosecuted or convicted.

Applicant was arrested, charged, and ultimately pleaded guilty to lesser charges resulting from her theft and credit-card fraud in 1990. I find that the stated disqualifying condition applies.

I have also considered all of the mitigating conditions for criminal conduct under AG ¶ 32 and considered the following relevant:

> (a) so much time has elapsed since the criminal behavior happened, or it happened under such unusual circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment; and
>
> (d) there is evidence of successful rehabilitation; including but not limited to the passage of time without recurrence of criminal activity, restitution, compliance with the terms of parole or probation, job training or higher education, good employment record, or constructive community involvement.

Appellant's crimes of theft and fraud back in 1990, when she was 20 years old, are remote and unique, qualifying for some mitigating consideration. However, full mitigation is not appropriate given Applicant's continuing untrustworthy behavior years later by taking computer equipment without proper authority and illegally downloading computer programs, music, and movies to include doing so from a government server without authorization. Her actions cast doubt on her reliability, trustworthiness, and judgment. AG ¶¶ 32(a) and 32(d) do not fully apply.

Guideline M, Use of Information Technology Systems

AG ¶ 39 expresses the security concern pertaining to use of information technology systems:

> 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 properly protect sensitive systems, networks,

> and information. Information Technology includes any computer-based, mobile, or wireless device used to create, store, access, process, manipulate, protect, or move information. This includes any component, whether integrated into a larger system or not, such as hardware, software, or firmware, used to enable or facilitate these operations.

AG ¶ 40 describes conditions that could raise a security concern and may be disqualifying. I have considered the following as potentially relevant:

> (e) unauthorized use of any information technology system.

Applicant downloaded thousands of computer media (music, movies, software programs, and games) between 1993 and 2011, to include doing so from a government server, without proper authorization. The above condition is applicable.

I reviewed all of the mitigating conditions under AG ¶ 41, and I considered the following relevant:

> (a) so much time has elapsed since the behavior happened, or it happened under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment.

Although some time has passed since Applicant engaged in her unauthorized action, and she initially accepted responsibility for her actions, more recently she has placed blame on the environment she was working in rather than her own behavior. Future recurrence cannot be ruled out. Without accepting responsibility for her actions her current reliability, trustworthiness, and judgment are called into question. AG ¶ 41(a) does not fully apply.

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 the 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 considered the potentially disqualifying and mitigating conditions in light of all the facts and circumstances surrounding this case. I considered the passage of time since Applicant's actions, her letters of recommendation and commendation, the testimony of her former supervisor, and her community involvement. However, what is most troubling about Applicant's behavior is that she possesses an extensive IT background, yet her inappropriate conduct fell directly into her area of expertise, i.e., theft of, or unauthorized use of computer hardware and software. Applicant failed to provide sufficient evidence to mitigate the personal conduct, criminal conduct, and use of information technology security concerns.

Overall the record evidence leaves me with questions and doubts about Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude Applicant failed to mitigate the security concerns under Guidelines E, J and M.

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
Subparagraphs 1.a – 1.c:	Against Applicant
Paragraph 2, Guideline J:	AGAINST APPLICANT
Subparagraph 2.a:	Against Applicant
Paragraph 3, Guideline M:	AGAINST APPLICANT
Subparagraphs 3.a – 3.c:	Against Applicant

Conclusion

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

_____
Robert E. Coacher
Administrative Judge