



**DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS**



In the matter of:)
)
) ISCR Case No. 18-00298
)
Applicant for Security Clearance)

Appearances

For Government: Chris Morin, Esquire, Department Counsel
For Applicant: Alan V. Edmunds, Esquire

10/31/2018

Decision

RICCIARDELLO, Carol G., Administrative Judge:

Applicant failed to mitigate the security concerns under Guideline E, personal conduct, Guideline H, drug involvement, and Guideline M, use of information technology. Applicant's eligibility for access to classified information is denied.

Statement of the Case

On February 15, 2018, the Department of Defense Consolidated Adjudications Facility (DOD CAF) issued to Applicant a Statement of Reasons (SOR) detailing security concerns under Guideline E, personal conduct, Guideline H, drug involvement, and Guideline M, use of information technology. The action was taken 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) effective within the DOD on June 8, 2017.

Applicant answered the SOR on March 15, 2018, and requested a hearing before an administrative judge. The case was assigned to me on June 28, 2018. The Defense

Office of Hearings and Appeals (DOHA) issued a notice of hearing on July 5, 2018. I convened the hearing as scheduled on August 14, 2018. The Government offered exhibits (GE) 1 through 4. As part of Applicant's answer to the SOR, she included Exhibits (EX.) A through M. At her hearing she testified and offered Applicant Exhibits (AE) A and B and EX A through M. There were no objections to any exhibits, and all were admitted into evidence. DOHA received the hearing transcript on August 22, 2018.

Procedural Matters

Applicant's counsel submitted a written motion and requested at the hearing that I recuse myself from the hearing. His documents and the Government's responses are attached as hearing exhibits. The motion was denied.¹

Findings of Fact

Applicant admitted SOR ¶ 1.a with an explanation. She partially admitted and denied SOR ¶¶ 1.b and 2.c. She denied SOR ¶¶ 2.a, 2.b, 2.d, and 3.a. She provided explanations for all of the allegations. After a thorough and careful review of the pleadings, exhibits, and testimony, I make the following findings of fact.

Applicant is 32 years old. She is not married. She is the mother of a ten-year-old son. She has some college education, but has not earned a degree. She served in the Army from 2005 to 2014, and was honorably discharged in the paygrade E-6. She worked overseas for a federal contractor from approximately May 2015 to May 2016. She was unemployed until she began working for her current employer in November 2016. She was hired to work in the network administration department, but is working on the help desk until the security clearance process is completed. She testified that she held a security clearance from 2005 until March 2016.²

In January 2016, Applicant completed a security clearance application (SCA). She signed it attesting to its accuracy. In May 2017, June 2017, and July 2017, Applicant was interviewed by a government investigator. She included the May 2017 summary of the personal subject interview (PSI) in her Answer to the SOR as evidence (AE J). Applicant was sent Government interrogatories that included the three PSIs (GE 2). The interrogatories requested that Applicant furnish full and truthful answers to the questions and sign the interrogatories under oath. The interrogatories advised Applicant to carefully review the PSIs and verify their accuracy. She checked "yes" (and initialed it) as to the accuracy of the information of the PSIs on the dates she was interviewed. She checked "yes" (and initialed it) that subject to additions or deletions, she adopted

¹ Hearing Exhibits (HE) I through IX are relevant to the motion. HE X and XI are Department Counsel's exhibit list and discovery letter, respectively. HE IX is attached to HE IV to be considered with the Government's brief.

² Tr. 9, 19-26, 43-44; GE 1, 2; Answer: EX. B, C, D, E, and G. While serving in the Army, Applicant was authorized to wear numerous campaign ribbons and other personal medals. GE 4 shows Applicant's loss of security clearance eligibility occurred when she separated from employment in May 2016.

the PSIs as accurately reflecting the interviews. She signed the document before a notary swearing (or affirming) its accuracy. She made a change to the date that was in the affirmation paragraph and printed "May 26, 2017" reflecting the accurate date of her first interview. In the copy of the PSI (AE J) that she introduced as evidence, she did not make changes to it or provide comments in her Answer to the SOR that there were inaccuracies or it was false.³

Applicant testified that when she received the Government's interrogatories she did not read them. She was only attesting to having had an interview. She claimed Department Counsel told her to sign the interrogatories and send them back. She said he did not tell her to verify the facts, but only to verify the interview took place. She said, "I called to verify exactly what needed to be done, if I needed to make any changes like spelling or grammatical errors or anything, and he was like, 'No, you're just verifying that the interview happened.'"⁴ Applicant then stated, "So basically just verify like I'm verifying that the interview had happened."⁵ She said Department Counsel did not say anything about the content of the document or what she should do.⁶

Department Counsel denied Applicant's version of that conversation. He said that he followed his standard format of what he tells all applicants and that is, he does not give legal advice; they should review the document; make whatever changes or corrections necessary to reflect its accuracy; and return it.⁷

Applicant testified that when she marked the interrogatories as accurate that it was false. When she signed the statement swearing to its accuracy, she testified that it was false. When she adopted the PSIs, subject to any additions or deletions, as accurately reflecting the interviews, she said that was also a false statement. She said she did not read the PSIs line by line and was unaware that she could make changes. Applicant did not make changes in the copy of the PSI she entered into evidence. She said she did not know she had the option of checking "no" instead of "yes." She thought the process would stop if she checked "no." She said after she had signed the interrogatories she asked people in the military security intelligence division where she worked about it. She said she did not ask advice before she signed it because she was in a hurry, and she did not think to do it. She testified that she made her corrections in her Answer to the SOR.⁸ Applicant's testimony was not credible.

³ Tr. 44-46, 67; GE 2; Answer EX. J.

⁴ Tr. 68.

⁵ Tr. 68.

⁶ Tr. 68-79.

⁷ Tr. 66-79.

⁸ Tr. 48-51, 66-79.

Applicant disclosed in her SCA that while in the Army she went to an Article 15 nonjudicial punishment in approximately July 2010. The SCA asked her to describe the Uniform Code of Military Justice (UCMJ) offense for which she was charged. Her answer was "UNKNOWN." Applicant disclosed during her May 2017 PSI that while deployed, she used someone else's computer credentials and password because she did not have administrative rights. She was the non-commissioned officer-in-charge of the information technology section at the time. She told the investigator that she was supposed to have administrative rights and access so she could fix network computer accounts for people while deployed, but it was not set up at the time, even though it was required in order for her to do her job. She explained that she used an account of a soldier, who worked for her and was an E-4 or below. She only used the account information in order to work on someone's account when they needed help. People in her unit knew this was occurring. After this information was made known to her superiors, she was reduced from staff sergeant to sergeant at an Article 15 hearing. She later earned her rank back. She advised the investigator that she was aware that using another person's account and password was not permitted, but she needed it in order to perform her job because access to her account had not been approved at the time.⁹

In Applicant's January 2016 SCA, which asked if she had "EVER" been charged with an offense involving alcohol or drugs, she answered "No." During Applicant's May 2017 PSI, she disclosed to the investigator that she had been charged with driving under the influence of alcohol (DUI) in March 2012.¹⁰ Applicant provided a letter from the attorney who represented her that stated they had appeared in court in January 2013. A not guilty verdict was entered by the judge.¹¹ Applicant was asked by the investigator why she did not disclose the DUI on her SCA as required. She stated that she was trying to hurry and complete the SCA, and thought when she was interviewed she could bring up the information, rather than list it in the SCA. She denied to the investigator that she was trying to hide the information.¹²

In Applicant's SOR answer, she explained the reason she did not disclose her 2012 DUI charge on her January 2016 SCA was because she was found not guilty and believed she did not have to disclose it. She stated in her SOR answer that she now understood she was required to disclose any charges, not just those where there was a guilty verdict. Applicant testified that the reason she failed to disclose the DUI in her January 2016 SCA was because she misunderstood the question. She did not

⁹ GE 2. This information was not alleged in the SOR. Any derogatory information that was not alleged will not be considered for disqualifying purposes, but may be considered when making a credibility determination, in the application of mitigating conditions, and in the whole-person analysis.

¹⁰ GE 2, 3.

¹¹ Answer: EX. K.

¹² GE 1, 2.

understand what “charge” meant. She did not commit the offense, so she did not think she had to disclose it. She now understands she should have disclosed it.¹³

In Applicant’s January 2016 SCA, which asked if she had “EVER” illegally used or otherwise been involved with a drug while possessing a security clearance, she answered “No.” Applicant answered “No” to all of the questions on the SCA regarding illegal drug use, including if she had used any in the past seven years. During Applicant’s May 2017 PSI, she disclosed to the investigator that she used marijuana in April 2015, while possessing a security clearance. She explained during the interview that she went to a friend’s bachelorette party, and her friend brought a chocolate bar laced with marijuana. Applicant ate a square of the chocolate. Applicant was consuming alcohol at the time. She told the investigator she did not have to pay for the marijuana. She noticed the effects of it as it made her jumpy and paranoid that she was going to get in trouble. She did not like the way it made her feel. She is no longer friends with those people who attended the party because they live far away from each other. When questioned by the investigator why she failed to disclose this information on her SCA, she said she was attempting to hurry and fill out the SCA to complete it, and she thought that when she was interviewed she would bring up the information, rather than put it in the SCA. She denied to the investigator that she was trying to hide the information. She did not tell the investigator that she ingested marijuana unknowingly.¹⁴

Applicant disclosed during her PSI to the government investigator that in either June or July 2016, she visited family in another state. While there she ate a brownie laced with marijuana that she got from her cousin. She was unemployed at the time, thought it was legal in the state where she used it, and she was not affected by it. She was consuming alcohol at the time. She did not have to pay for the marijuana. Her cousin and other family members who were present were aware of her use. She did not have a security clearance at that time.¹⁵

Applicant explained to the investigator that the reason she used marijuana on the two occasions mentioned in 2015 and 2016 was because she wanted to try it in that form. She told the investigator, she had not used any illegal drug, including marijuana, in the past seven years, except for the two times mentioned.¹⁶

Applicant testified that she used marijuana in April 2015 while holding a security clearance, but said she used it unknowingly. She said while attending the bachelorette party she was given candy, and she did not know it had marijuana in it. She later learned from people attending the party that the candy had marijuana. She said she has never knowingly used any illegal drug. She has taken random drugs tests in the military

¹³ Tr. 34-35, 55.

¹⁴ GE 1, 2.

¹⁵ GE 2.

¹⁶ GE 2.

and as a civilian with negative results. She provided the results of drug tests from March 2018 (two different weeks), July 2018 and August 2018 that showed negative results for illegal drugs.¹⁷

Applicant stated in her Answer that the reason she failed to disclose her drug use while holding a security clearance in her January 2016 SCA was because she believed she only had to disclose information if she had been found guilty in a court of law. She testified that the reason she failed to disclose this drug use was due to an “honest mistake.”¹⁸

Applicant denied she told the investigator that she knowingly used marijuana in April 2015 while holding a security clearance. She testified this was a misunderstanding. She said at the time she consumed the candy, she did not know it was laced with marijuana.¹⁹

In Applicant’s Answer, she admitted using marijuana around June or July 2016, but said she did not hold a security clearance at the time as she was unemployed. She stated in her Answer that she regretted her conduct and has not used marijuana since then. She did not say her use was unknowing. At her hearing, Applicant testified that she used marijuana in June or July 2016 unknowingly. She said she did not hold a security clearance in June 2016. She did not recall the circumstances of the use; did not recall how she learned the brownie and candy contained marijuana; and did not recall who told her the items contained marijuana. She admitted that she consumed the marijuana in both instances, but denied she was aware that the brownie and candy contained marijuana until after the fact.²² Applicant’s Answer to the SOR stated:

Furthermore, this behavior was fully admitted during my personal subject interview. I regret my actions during this time and I have not used an illegal substance since 2016, a period of almost two years, and have no desire.²³

During the May 2017 interview, Applicant told the investigator that when she was working for her employer from November 2016, she had not been approved at that time for a security clearance, and she did not have an interim clearance. Her coworkers and supervisors were aware she did not have a clearance. She was assigned to the call center help desk. She explained that she received calls for both unclassified and Secret clearance level computer issues. She stated that most calls were for issues with the Secret computer systems. When she began working at the help desk, she transferred

¹⁷ Tr. 26-31, 33, 46; AE B; Answer: EX. L.

¹⁸ Tr. 35; Answer to SOR.

¹⁹ Tr. 49.

²² Tr. 31-34, 79-80; Answer to the SOR.

²³ Tr. 79-83; Answer to the SOR.

the calls for customers that had Secret computer system issues to other coworkers who had the appropriate clearances. She brought up this topic with her supervisor, advising the supervisor that Applicant did not have a SIPR token, which is a classified computer access card, and that Applicant was unable to help customers with classified computer issues. She further told the investigator that through natural progression, without much discussion, she was allowed access to her coworkers' computer stations by having the coworker enter their tokens and passwords when Applicant received a call from someone through the help desk that was using a classified computer. She told the investigator that she was actually performing the function under the coworkers' usernames and has also done this under her supervisor's username at his desk. She was able to do this when her coworkers or supervisor were not using their classified computers because access was limited to one user at a time.

Applicant explained to the investigator that at the call center each employee has three computers at their work station. One is unclassified, one is classified, and the third is CIE, another unclassified system. She did not know what the abbreviation stood for. Applicant only had access to the unclassified and CIE computers at her work station. She further explained that when someone called for help and they had an issue on a classified system, she was not able to help them using her credentials. So, while her coworkers were on the phone with someone and they were using one of their unclassified computers, she would go to a coworker's work station and the coworker would enter their token to access their classified computer along with their password, and then Applicant used their classified computer to assist the person with their classified computer issues. She stated that she was not permitted to have access to the Secret classified system or the building. She believed the officer-in-charge had seen her in the building and was aware she did not have the proper clearance to be there. She did not think the officer-in-charge knew her coworkers and supervisor had given her access to the classified computer system by allowing her to login with their usernames and passwords. She told the investigator that she was aware that she was not supposed to use her coworkers' computers. She explained that she would not be able to do her work if she did not have access to her coworkers' classified computers. She needed her job to pay bills while she was waiting for her clearance.²⁵

Applicant testified that she explained to the investigator that she worked in the help center and received calls requiring access to classified computers. She would pass these calls to her coworkers who had access. She said she was unable to help customers who had issues with their classified computers. She testified that she was never informed that her clearance was suspended. She testified it was a misunderstanding that she personally accessed classified computers. She denied she accessed classified computers. She said she would ask a coworker to assist a customer who had problems with their classified computer. She denied that she ever used someone else's credentials to accessed classified information. There was no official action taken against Applicant for her conduct. Applicant testified that she did not

²⁵ GE 2.

access classified computers without proper authorization. She said the investigator misunderstood her when he indicated this in his report.²⁶

During the interview with the government investigator, Applicant was asked by the investigator why she had brought her cell phone into a facility that was marked on the door to the building “no personal electronic devices” (PED) allowed. This issue came up when during this interview, which took place in the secure building, Applicant referred to information from her cell phone. She told the investigator that she normally does not bring her cell phone to work, but because no one was at work that day, she brought it with her. Applicant also explained that the area where this interview took place was an unclassified area, even though it was in the building with the sign that prohibited PEDs. She said that she normally leaves her cell phone in her car or in the cell phone lockers just inside of one of the building entrances. Applicant stated that she did not bring her cell phone to work and use it because there were random scans for PEDs. She admitted to the investigator that it was wrong to bring her cell phone into work the day of her interview, and she did not normally do it.²⁷

Applicant testified that she brought her cell phone into a building that had a sign outside prohibiting PEDs. She said she told the government investigator during the interview that she had information on her cell phone. She testified that the investigator told her to retrieve the phone to get the information and Applicant did. Applicant stated she was not in a secure area at the time. This contradicts the PSI that says the investigator asked her why she had brought her cell phone into a secure facility during her interview.²⁸

Applicant testified that when she completed the January 2016 SCA she was in a hurry to complete the form. She knew she would be interviewed. Understanding that many questions require a “yes” or “no” answer, she did not have an explanation for why checking the accurate answer would take more time. She stated she wanted an opportunity to provide explanations for certain questions on the SCA.²⁹

Applicant’s testimony was not credible. She deliberately omitted material facts on her January 2016 SCA when she failed to disclose her March 2015 marijuana use while holding a security clearance. She knowingly brought her cell phone into a building where PEDs were prohibited. Since about November 2016, she knowingly and repeatedly, without holding a security clearance, intentionally used other employees’ access credentials to gain unauthorized entry to classified computer systems and networks at the command where she provided information technical support.

²⁶ Tr. 38-40, 60-63.

²⁷ Tr. 65-66; GE 2.

²⁸ Tr. 35-38, 64-65.

²⁹ Tr. 53-55, 57-59, 84.

Applicant provided a statement of her intent not to use illegal drugs in the future and agrees to the revocation of a security clearance if she fails to abide by her intention. She provided character letters. In them, she is described as loyal, trustworthy, exceptional, serious, reliable, honest, courageous, ambitious, generous, resilient, respectful, dignified, motivated, patient, professional, competent, hard-working, and valued. She is involved in her community. She provided copies of certifications she has completed. She also provided a copy of her 2012-2013 enlisted evaluation.³⁰

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(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 access to classified information will be resolved in favor of 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. Likewise, I have not drawn inferences grounded on mere speculation or conjecture.

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 the applicant may deliberately or inadvertently fail to safeguard

³⁰ Answer: EX. A, B, F, and I.

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 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).

Analysis

Guideline H: Drug Involvement and Substance Misuse

The security concern relating to the guideline for drug involvement and substance misuse is set out in AG ¶ 24:

The illegal use of controlled substances, to include the misuse of prescription and non-prescription drugs, and the use of other substances that cause physical or mental impairment or are used in a manner inconsistent with their intended purpose can raise questions about an individual’s reliability and trustworthiness, both because such behavior may lead to physical or psychological impairment and because it raises questions about a person’s ability or willingness to comply with laws, rules, and regulations.

AG ¶ 25 provides conditions that could raise security concerns. The following are potentially applicable:

- (a) any substance misuse;
- (c) illegal possession of a controlled substance, including cultivation, processing, manufacture, purchase, sale, or distribution; or possession of drug paraphernalia; and
- (f) any illegal drug use while granted access to classified information or holding a sensitive position.

There is sufficient evidence that Applicant knowingly used marijuana in March 2015, while holding a security clearance. After she completed her SCA in January 2016, she again used marijuana in June or July 2016. In order to use it, she had to possess it. There is sufficient evidence to establish the above disqualifying conditions.

The guideline also includes conditions that could mitigate security concerns arising from financial difficulties. The following mitigating conditions under AG ¶ 26 are potentially applicable:

(a) the behavior happened so long ago, was so infrequent, or happened under such circumstances that it is unlikely to recur or does not cast doubt on the individual's current reliability, trustworthiness, or good judgment; and

(b) the individual acknowledges his or her drug involvement and substance misuse, provides evidence of actions to overcome the problem, and has established a pattern of abstinence, including, but not limited to:

(1) disassociation from drug-using associates and contacts; (2) changing or avoiding the environment where drugs were being used; and (3) providing a signed statement of intent to abstain from all drug involvement and substance misuse, acknowledging that any future involvement or misuse is grounds for revocation of national security eligibility.

Applicant knowingly used marijuana while holding a security clearance in 2015. After completing her SCA in January 2016, she again used marijuana in June or July 2016. She did not hold a security clearance at that time. Applicant says she no longer associates with people who use illegal drugs and provided a letter of intent to not use drugs in the future. These facts weigh in Applicant's favor. However, her 2016 use was with a family member. It is unknown whether she will disassociate herself from him. The concern is that Applicant held a security clearance when she used marijuana in April 2015. She admitted to the investigator the details of her 2015 use. Later she denied her use was knowing. She admitted to the investigator that she used marijuana in 2016 with her cousin, and then denied it was knowing. This second use took place after she completed her SCA and was on notice of the importance of not using illegal drugs. I find that her behavior casts doubt on her current reliability, trustworthiness, and good judgment. She does not acknowledge her drug involvement, but apparently has disassociated herself from friends who use drugs. AG ¶ 26(a) does not apply. AG ¶ 26(b) has some application, but it is not sufficient to overcome the security concerns raised under this guideline.

Guideline E: Personal Conduct

AG ¶ 15 expresses the security concern for personal conduct:

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. The following will normally result in an unfavorable national security eligibility determination, security clearance action, or cancellation of further processing for national security eligibility:

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

(a) deliberate omission, concealment, or falsification of relevant facts from any personnel security questionnaire, personal history statement, or similar form used to conduct investigations, determine employment qualifications, award benefits or status, determine security clearance eligibility or trustworthiness, or award fiduciary responsibilities;

(d) 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; 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.

There is sufficient evidence that Applicant knowingly used marijuana while holding a security clearance. There is sufficient evidence that Applicant deliberately omitted her prior drug use on her January 2016 SCA, as alleged in SOR ¶ 2.b.

The PSI is detailed and specific in which Applicant provided a step-by-step explanation to the government investigator regarding her drug use; her unauthorized conduct in gaining access to the command classified computer system; and her failure to disclose information she was required to on her SCA. She testified that the reason she failed to disclose the information alleged in her SCA was because she wanted to explain it during the government interview. She took that opportunity to explain her actions. It is not believable she was unaware of the contents of the PSI and that the investigator misunderstood numerous statements she made regarding her conduct as alleged. AG ¶ 16(a) applies.

There is sufficient evidence that Applicant knowingly brought her personal cell phone into a building where PEDs are prohibited. There is sufficient evidence that beginning in November 2016, Applicant knowingly, without holding a security clearance, intentionally used others' credentials to gain unauthorized entry to the classified computer systems and networks at a command where she provided information technology support. AG ¶¶ 16(d) and 16(e) apply to SOR ¶¶ 2.c and 2.d.

Applicant's explanation that because she was found not guilty to the 2012 DUI charge, she mistakenly believed she did not need to disclose it on her January 2016

SCA, and she was confused about the differences between being charged and convicted, was somewhat credible. There is insufficient evidence to conclude she deliberately omitted this information. I find in her favor for SOR ¶ 2.a.

After the Government produced substantial evidence of those disqualifying conditions, the burden shifted to Applicant to prove mitigation. The following mitigating conditions under AG ¶ 17 are potentially applicable to the disqualifying security concerns based on the facts:

- (a) the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts;
- (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 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.

There is insufficient evidence to conclude Applicant made a prompt good-faith effort to correct the omissions before being confronted with the facts. She provided inconsistent and contradictory explanations for her conduct in her Answer to the SOR, the PSI, and her testimony. None of her actions were minor or infrequent, but rather there is considerable evidence and a pattern of behavior that cast doubt on Applicant's reliability, trustworthiness, and good judgment. AG ¶¶ 17(a) and 17(c) do not apply.

Applicant has not acknowledged her behavior. She gave the investigator a detailed account of how she did not have authorization to access the classified computer system, but gained access by using coworkers' credentials with their permission. She brought her cell phone into a secure area against the rules. She then denied all of her past admissions during her testimony. I cannot find that AG ¶¶ 17(d) or 17(e) apply.

Guideline M: Use of Information Technology

The security concern relating to the guideline for drug involvement and substance misuse is set out in AG ¶ 39:

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 provides conditions that could raise security concerns. The following are potentially applicable:

- (a) unauthorized entry into any information technology system; and
- (e) unauthorized use of any information technology system.

There is sufficient evidence that Applicant intentionally used other employees' access credentials to gain unauthorized entry to the classified computer system and network at the command where she provided information technology support. While working at the help desk, when a call came in for assistance that involved a classified computer, her coworkers used their credentials to access a classified computer and then allowed Applicant to work on the classified computer, without proper authorization, to assist the customer. The above disqualifying conditions apply.

The guideline also includes conditions that could mitigate security concerns. The following mitigating conditions under AG ¶ 41 are potentially applicable:

- (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;
- (b) the misuse was minor and done solely in the interest of organizational efficiency and effectiveness;
- (c) the conduct was unintentional or inadvertent and was followed by a prompt, good-faith effort to correct the situation and by notification to appropriate personnel; and
- (d) the misuse was due to improper or inadequate training or unclear instructions.

Applicant's conduct was not a one-time occurrence. Beginning in November 2016, she repeatedly worked on classified computers using the credentials of coworkers. Her explanation was she needed to do this so she could assist those customers who had problems with their classified computers. Otherwise she was unable to assist them because she had not yet been granted the necessary credentials. The

misuse was not minor, but recurring. There is no evidence that she was attempting to do anything other than help the customers. She intentionally violated the rules and regulations. Applicant has been a part of the information technology program since she served in the Army. There is no evidence that her actions were inadvertent or that she was unaware of the proper protocol. Applicant knew she was not authorized to access classified computers until after she had the proper clearance. She was aware that working on a classified computer without the proper clearance was prohibited, and that it was wrong to use coworkers' credentials, even with their permission. None of the mitigating conditions 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 relevant circumstances. The administrative judge should consider the nine adjudicative process factors listed at AG ¶ 2(a):

(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 have incorporated my comments under Guidelines H, E, and M in my whole-person analysis. Some of the factors in AG ¶ 2(a) were addressed under those guidelines, but some warrant additional comment.

Applicant is a 32-year-old Army veteran. She knowingly used marijuana while holding a security clearance. After submitting her SCA in January 2016, she used marijuana again. Applicant provided different explanations in her PSI, Answer to the SOR, and testimony for why she failed to disclose required information on her SCA. Applicant did not have a security clearance when she deliberately and repeatedly worked on classified computers using coworkers' credentials to gain unauthorized entry. Applicant was disciplined while in the Army for similar conduct. Her testimony was not credible and inconsistent with prior accounts. Overall, the record evidence leaves me with serious 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 arising under the drug involvement, personal conduct and use of information technology guidelines.

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 H:	AGAINST APPLICANT
Subparagraphs 1.a-1.b:	Against Applicant
Paragraph 2, Guideline E:	AGAINST APPLICANT
Subparagraph 2.a:	For Applicant
Subparagraphs 2.b-2.d:	Against Applicant
Paragraph 3, Guideline M:	AGAINST APPLICANT
Subparagraph 3.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 national interest to grant Applicant a security clearance. Eligibility for access to classified information is denied.

Carol G. Ricciardello
Administrative Judge