DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 19-02773
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Adrienne Driskill, Esq., Department Counsel
For Applicant: *Pro se*

December 6, 2021

_____

Decision

_____

GLENDON, John Bayard, Administrative Judge:

Applicant has failed to mitigate security concerns regarding drug involvement and use of information technology. Based upon a review of the pleadings, the documentary evidence, and Applicant's testimony, national security eligibility for access to classified information is denied.

Statement of the Case

On December 9, 2015, Applicant submitted a security clearance application (SCA). On November 27, 2019, the Defense Counterintelligence and Security Agency, Consolidated Adjudications Facility (CAF), issued a Statement of Reasons (SOR) to Applicant detailing security concerns under Guideline H (Drug Involvement and Substance Misuse) and Guideline M (Use of Information Technology). The CAF acted under Executive Order 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended (Exec. Or.); Department of Defense (DoD) Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the adjudicative guidelines (AG) promulgated in

Security Executive Agent Directive 4, *National Security Adjudicative Guidelines* (December 10, 2016), effective within the DoD on June 8, 2017.

On January 14, 2020, Applicant provided a written response to the SOR (Answer). He supplemented his Answer July 6, 2021, to more specifically respond to one of the SOR allegations (Supplemental Answer). He requested a hearing before an administrative judge of the Defense Office of Hearings and Appeals (DOHA). On September 10, 2021, the case was assigned to me. DOHA issued a hearing notice on September 15, 2021, scheduling the hearing for October 20, 2021.

I convened the hearing as scheduled. Department Counsel presented Government Exhibits (GE) 1 and 2, which were admitted without objection. Applicant had prepared a document for submission, but left it at his residence. I kept the record open until October 27, 2021, to give Applicant the opportunity to supplement the record. He timely submitted three additional documents, which I marked as AE A through C and admitted into the record without objection. DOHA received the hearing transcript (Tr.) on October 27, 2021.

Findings of Fact

Applicant's personal information is extracted from his SCA unless otherwise indicated by a parenthetical citation to the record. After a thorough and careful review of the pleadings, Applicant's testimony, and the documentary evidence in the record, I make the following findings of fact.

Applicant is 49 years old and has worked for a DoD contractor as a systems engineer since 2014. He has a high school diploma and has earned a number of professional certifications. He married and divorced once as a young man. He subsequently cohabited with a woman for a number of years and married her in 2008. He has an adult stepchild. (Tr. at 21, 35.)

After graduating from high school in 1991, Applicant enlisted in the U.S. Air Force with the intent to serve until his mandatory retirement. He wrote in his SCA that he was discharged in April 1993 under "General Honorable Conditions." He then wrote "Discharge Detail Other Than Honorable," suggesting that the character of his discharge was Under Other Than Honorable Conditions." He also wrote in his SCA that the reason for his discharge was a "Reduction in forces." He provided the same reason at the hearing. (SCA at18; Tr. at 22.)

In his May 2019 background interview (2019 Interview), Applicant disclosed that he was discharged for misconduct. The only detail he said he could recall was the phrase conduct prejudicial to good order and discipline. In an April 2016 background interview (2016 Interview), Applicant was more forthcoming about his military discharge. He disclosed that he received a letter of reprimand in January 1993 for disrespecting a superior and served a day, but not overnight, in the Correctional Custody Unit. He had also been repeatedly counseled for dereliction of duties and for a poor attitude. On two occasions, he received letters of counseling for dereliction of duties. He blamed his

superior officer for treating him differently than others due to his religious faith. In the 2016 Interview, he claimed he was told that he was being released under a reduction in forces separation process. (2019 Interview at 6; 2016 Interview at 13.)

Applicant attended a class at a junior college when he was a senior in high school. During the period August 1995 to May 1997, Applicant attended a tech school and earned two IT certificates of completion. In subsequent years, he was awarded additional IT certifications, mostly through self-study. Since 2014 or 2015, he has worked for a Federal contractor as a systems engineer. He held a security clearance when he served in the Air Force. He was not granted an interim security clearance after submitting his SCA in 2015. His employer would like Applicant to have a clearance so that he could work on classified matters, but he can continue his employment at his company without a clearance. It would be helpful to both his employer and Applicant if he had a clearance to work directly on classified contracts rather than around the perimeter in an unclassified environment. (SCA at 13; Tr. at 20, 22-24, 27-32.)

SOR Allegations

Paragraph 1, Guideline H, Drug Involvement and Substance Misuse

In his Answer, Applicant admitted the facts alleged in the two subparagraphs of the SOR under this guideline. In his Supplemental Answer, he specifically denied the allegation in SOR ¶ 1.b. The specific facts regarding each of the allegations are as follows:

1.a – Use of marijuana in April and May 2019 – In his 2019 Interview, Applicant reported that he was given an item sample containing ingredients made from cannabis by a vendor at an April 2019 Earth Day event. This occurred about a month before the interview. He consumed the product thinking it was a candy and not knowing it was a marijuana edible (Edible). This was the first time he ever consumed "marijuana," using that term broadly to include all products derived from marijuana. At the event, which is generally associated with marijuana, Edibles were for sale. Applicant claimed that the item he consumed was not labeled to show that it contained marijuana. He later learned that he had consumed an Edible. He testified it was not his intent to consume marijuana or a marijuana product when he attended this event. (Tr. at 36-39; GE 2 at 9.)

In his 2019 Interview, Applicant further reported that his wife subsequently purchased more Edibles at a cannabis dispensary in Applicant's home state where the sale of such products is legal under state law. Applicant deliberately consumed Edibles a few more times after his first experience with Edibles. At the time of the 2019 Interview on May 21, 2019, he was still consuming Edibles. He said that was taking the Edibles to ease shoulder pain and to sleep better at night. He intended to see his doctor in the near future "to get a note for this." At the time of the Interview, Applicant acknowledged that he was aware that Edibles were not legal under Federal law. (GE 2 at 9.)

Applicant provided additional information in his October 2019 responses to DOHA's Interrogatories about his past use of Edibles. He confirmed the accuracy of the

report of his 2019 Interview regarding his past drug use and adopted the statements contained in the report. He also wrote:

> I would like to ensure clarification that this [past use of edibles] was a rather desperate occurrence due to my shoulder pain preventing me from sleeping and this was only done after several (4-5) days of (almost) no sleep due to the shoulder pain.
>
> Hence forth [sic] I have resorted to the prescription medications for pain as prescribed by my doctor despite the negative effects associated.

He also corrected a statement in the report of the 2019 Interview, noting that: "The strength of the product in question, while 10 mg per standard dose, was divided and was not 15mg [as written in the report]. The approximate dosing was 2.5-5 mg." (GE 2 at 3-4, 19, 21-22.)

In his January 2020 Answer, Applicant confirmed that he consumed Edibles in April and May 2019 to help him sleep after "excessive periods of time when [he was] unable to sleep." He wrote that his decision to consume Edibles was made out of "desperation." He wrote further:

> I have, as intended, engaged with my primary care physician in exploring FDA approved medications to assist with my incremental sleep problems. My primary care physician and I are exploring medications to resolve sleep issues that do not leave lingering effects the following day that could potentially affect my work performance.

Answer at 1.

At the hearing, Applicant explained that he consumed the Edibles in 2019 under extraordinary circumstances. He experienced significant pain in his shoulder due to a work-related injury and was unable to sleep for about three days. He ate the Edibles to help him sleep on two or three occasions while he was waiting to see his workers' comp doctor. He made a point that he only used a "quarter" of the "standard dosing" in the square Edible and that his use was infrequent and an "isolated incident." He waited "a very short period of time" to see his workers' comp doctor, an orthopedist. The doctor gave Applicant a prescription for his pain. The medication helped him sleep without using the Edibles. He also made a comment about how long it takes to be seen by a workers' comp doctor, which was inconsistent with his earlier testimony that he had an appointment with that doctor after only waiting a short time. Also, he provided no testimony regarding his primary care physician or that doctor's role in "exploring medications" with Applicant. (Tr. at 40-50, 56.)

Applicant has not used Edibles since May 2019, the month of his 2019 Interview. During the period when he was unable to sleep, Applicant did not consider the option of seeing a doctor at a 24-hour healthcare facility. Applicant believed that was not a viable

option because he assumed that this type of doctor would tell him to take Tylenol for his pain. He did not believe that an over the counter drug like Tylenol would be sufficiently helpful for his condition. Applicant confirmed at the hearing that he knew at the time he consumed the Edibles that it was not legal to do so under Federal law and that it was against his employer's drug policy. He also confirmed that he understood that at the time of his use of the Edibles, he was under consideration for a security clearance. In explaining his thought process at the time he consumed the Edibles, he provided a curious analogy between marijuana and alcohol, stating that they have "pretty much the same restrictions" and both are "controlled." He made the same point in his post-hearing submission (AE A), writing that: "edibles are available to the general public in an over the counter fashion just like alcohol." He noted at both the hearing and repeated in AE A his wife had leftover prescription pain medication and that he chose not to take the medication since the prescription was not written for him. He commented in AE A that "prescription pain killers are controlled substances that are not publicly available in an over the counter fashion, like alcohol." He argued that he made the better choice by using Edibles, not the leftover pills, to relieve his pain. Applicant was unaware at the hearing that marijuana is a Schedule I controlled substance under the Federal Controlled Substances Act, even though, as noted, he knew that marijuana was illegal under Federal law. (Tr. at 45, 48-50, 54-56; AE A at 2.)

1.b – Expressed intent to continue using marijuana in the future – In his 2019 Interview, Applicant also made the statement that he may consider taking Edibles in the future if needed for pain. He advised that he was going to see his doctor in the near future and to get a "note" for using Edibles. In response to the Government's interrogatories, Applicant was given the opportunity to correct any errors in the report of his 2019 Interview, and he made a number of corrections. None of his corrections addressed his comments about his intention to use Edibles in the future. (GE 2 at 9, 18-20.)

In his Answer, Applicant explained that his comment about future use made during his 2019 Interview was made "with the caveat of only under extreme circumstances, such as having not slept for upwards of 72 hours, and only in the event of a delay in interacting with my primary care physician to help resolve the problem." He wrote further:

> Since the time of my interview no further use has occurred as my primary care physician was able to see me in a very expedited manner and begin addressing the problem.

Answer at 1. In his Supplemental Answer, Applicant specifically answered SOR allegation in subparagraph 1.b by stating: "I deny that I have intent to use marijuana in the future." (Supplemental Answer at 1.)

At the hearing, Applicant discussed further the "note" he wanted his doctor to provide, which he discussed in his 2019 Interview. He explained that he wanted the doctor to write "something to state that it was a pertinent solution to the immediate problem," that being his lack of sleep due to shoulder pain. He explained further that the note should address that Applicant's use of edibles was "a last-minute desperate solution to an

impossible problem." He did not provide such a note from his doctor or any doctor. Applicant no longer believes that he will ever use an illegal drug again because he has his shoulder pain under control with medications, when needed. He also reaffirmed his denial of the allegation regarding future intent to use illegal drugs. (Tr. at 47, 50-51, 56-60.)

During closing argument, Applicant and I engaged in a lengthy discussion about his failure to provide a signed statement pursuant to AG ¶ 20(b)(3) that set forth both his intent to abstain from using illegal drugs in the future and an acknowledgment that any future drug use by him would be grounds for the revocation of his national security eligibility. He said he did not submit such a statement because he expected the Government to provide him with an appropriate form for that purpose. After the hearing, he provided a signed statement of his intent to abstain from any future drug use. He also wrote: "Additionally, I do understand that these infractions are grounds for revocations of security clearances issued by the U.S. government." (Tr. at 105-111; AE C.)

Paragraph 2, Guideline M, Use of Information Technology

In his Answer, Applicant admitted the facts alleged in the one subparagraph of the SOR under this guideline. The specific facts regarding this allegation are as follows:

2.a – Purchase and use in August 2015 of an external USB WiFi card –

Applicant answered the following question in his SCA in the affirmative:

Section 27- Use of Information Technology Systems

Unauthorized Access
In the last seven (7) years have you illegally or without proper authorization accessed or attempted to access any information technology system?

In response to the follow-up questions in his SCA, Applicant disclosed that in August 2015 he "purchased an external USB WiFi card while at Defcon [sic] and have been learning how to use Kali Linux."

At his 2016 Interview, Applicant discussed the above admission in his SCA. He stated that in addition to the two items described, he also purchased a directional antenna. He said that these items are typically used to break into password-protected wireless internet networks. The antenna can be aimed to receive WiFi signals as far away as two miles. He explained that Kali Linux is software used to overcome password protection on WiFi systems. He admitted that the unauthorized entry of a secure computer system would be a violation of law. He has never tried to access the WiFi system of a corporate computer system. He has only attempted to enter WiFi systems that appear to him to belong to individuals. He believed that entering the network of a private party would be a

lesser violation of secularity restrictions. In response to a separate question in DOHA's interrogatories, he acknowledged as correct the following statement:

> 1. In August 2015, you purchased an external USB WiFi card and have used it at various [he corrected the word "various" by inserting "1 (one)"] locations attempting to break into password protected wireless internet networks.

He then advised that his attempts using his hacking equipment were never successful and that his last attempt was made in August 2015. (GE 2 at 15-16, 24.)

Applicant also reported in his 2016 Interview that he has taken the equipment to parties at homes of his friends and has allowed them to use the equipment. He said he does not recall if any of his friends were able to enter a secure WiFi network, but he was not certain of that. (GE 2 at 15.)

In his October 21, 2019 responses to DOHA's interrogatories, Applicant was given the opportunity to correct any errors in the reports summarizing his 2016 and 2019 Interviews. He made a few minor corrections, but made no changes to the portions of the 2016 Interview report summarized above. He then affirmed that the interview summaries attached to the Interrogatories were accurate as corrected and adopted the statements. He signed his interrogatory responses before a Notary Public. (GE 2 at 4, 25-26

At the hearing, Applicant provided extensive testimony about his involvement in DEFCON and his purchase and use of the hacking equipment. Applicant and his wife have attended an annual IT security conference call DEFCON since 2010 or 2011. They became volunteer staff members of DEFCON in about 2015. The conference is an important venue for IT security professionals to stay current on developments in their field. (Tr. at 29-33.)

Applicant testified that in 2015, at the DEFCON conference in Las Vegas, he purchased an external USB WiFi card, which gets plugged into a computer and can be used to identify WiFi networks available in the area for connection. He explained that all computers and phones use an internal WiFi card to perform this function. The external card he bought not only has a USB connection to connect to a computer, it also has an antenna port that is used to connect to an external antenna. That is the only difference of the external WiFi card he purchased. The card he purchased came with an antenna. As a staff member of DEFCON, he purchased the equipment at a discounted price. With the addition of an antenna, he is able to conduct a directional search for available WiFi networks. He testified that he purchased the equipment for "continuing education." Quoting Sun Tzu, he wanted to "know thy enemy," meaning that he wanted to better understand the capabilities of hackers who use this type of hacking equipment to break into computer networks. He wanted to use the hacking equipment to see if he could gain access to password protected networks. To get through a password protection WiFi network, he needed to download a "suite" of software called Kali Linux and use one of the programs in the suite. (Tr. at 62-71.)

Applicant explained that he was never successful hacking into a password protected network with his hacking tools and software. In the process of trying, he was learning how the tools work. He blamed his lack of success on his lack of expertise working with Linux software. He attempted to use the tools at his apartment after the conference. The antenna had a stated range of two miles, but Applicant explained that the quality of the data transmission was poor at longer distances. His next-door neighbor's WiFi network would certainly be within reach of the antenna and software. He initially claimed he used the hacking tools over a day or two, but then he immediately modified this statement saying he limited his use to one time for 30-45 minutes before dinner time. When asked if he had used the hacking equipment since that time, he responded: "Not to my recollection." He also limited the target networks into which he sought to gain entry. He testified that he only "picked something that said 'guest.'" Subsequently, Applicant tried to explain what he meant by the word "guest" as something different than a business owned and managed WiFi system. In his post-hearing submission, he repeated his claim that he only "selected for testing networks containing 'Guest' in their SSID [Service Set Identifier or wireless network name]," and he did "not believe . . . [that] would be considered problematic." He also repeated his position that his activities were merely self-education in matters "that are used for nefarious activities." He was simply "striving to maintain a sufficient level of education to improve this facet of my IT responsibilities." (Tr. at 72-76, 78, 86-90, 93; AE A at 1.)

Applicant also testified that his self-education with the hacking equipment was never a part of any work-related project for his employer. He explained that he is "not part of that team" that works on accessing password-protected WiFi networks. When asked if he understood the Government's security concerns regarding the illegality of trying to access password-protected networks without authorization, Applicant responded, "I understand that there is verbiage about it." When asked if he has any aspirations to be a hacker, he responded:

> "Hacker" is a lot of different terms . . . Everyone is a hacker if you think about it. You know, you talk - - at Starbucks, you talk somebody into giving you, Hey, can you give me an extra shot of espresso, Matt, would you? That type of thing is hacking.

(Tr. at 80-82.)

Applicant also testified that most of his friends who work in IT positions are far more knowledgeable than he is with respect to security matters. He agreed that he "may have taken [the hacking tools] to a get-together [with his IT friends] once . . . I don't know if anyone used it or not." He then testified "I'm going to assume no one picked it up and messed with it." (Tr. at 76-77.)

Applicant was asked if he agrees that accessing password-protected networks is illegal. He responded as follows:

> I would imagine there is something written somewhere about it. As I am not a lawyer for the EFF [Electronic Frontier Foundation], I can't be much more specific than that.

He also testified that he sought to limit the targets of his attempted hacking activity. He said:

> I don't know what the rules are about networks that are labeled as "guest" that are intended for guest access, that are segregated from internal corporate network that actually contain pertinent business and financial data . . . Thus, my decision to pick something that said "guest."

(Tr. at 77-78.)

Whole-Person Evidence

After the hearing, Applicant provided four character letters, which have been marked collectively as AE B. They describe him as trustworthy, dependable, loyal, and a good friend. His references believe that he is highly professional and a person of integrity. His performs high-quality work and receives outstanding annual reviews. His most recent character letter is dated April 2, 2018, from his supervisor at the time. He also produced a November 2017 report from the FBI that stated that it found no record of Applicant having ever been arrested. (AE B at 1-5.)

The subject line of the April 2, 2018 character reference letter reads: "Recommendation for military discharge characterization upgrade for [Applicant]." The conclusion of the letter in the penultimate paragraph states:

> Given his drive for excellence and superb character, it is my professional recommendation that [Applicant] have his military discharge characterization upgraded to Honorable."

Applicant provided no evidence as to whether his discharge upgrade petition was granted. (AE B at 5.)

Applicant testified at length that he has a unique set of skill sets that makes him a valuable member of his employer's team. Most of his colleagues are experts in Linux, while Applicant has a different expertise making his skillset unique. Much of his technology knowledge is self-taught. (Tr. at 30-34.)

Policies

"[N]o one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988). As Commander in Chief, the President has the authority to "control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to have access to such information." *Id.* at 527. The President has authorized the Secretary of Defense or his designee to grant applicants eligibility for access to classified information "only upon a finding that it is clearly consistent with the national interest to do so." Exec. Or. 10865 § 2.

Eligibility for a security clearance is predicated upon the applicant meeting the criteria contained in the adjudicative guidelines. These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, an administrative judge applies these guidelines in conjunction with an evaluation of the whole person. An administrative judge's overarching adjudicative goal is a fair, impartial, and commonsense decision. An administrative judge must consider all available and reliable information about the person, past and present, favorable and unfavorable.

The Government reposes a high degree of trust and confidence in persons with access to classified information. This relationship transcends normal duty hours and endures throughout off-duty hours. 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.

Adverse clearance determinations must be made "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." Exec. Or. 10865 § 7. Thus, a decision to deny a security clearance is merely an indication the applicant has not met the strict guidelines the President and the Secretary of Defense have established for issuing a clearance.

Initially, the Government must establish, by substantial evidence, conditions in the personal or professional history of the applicant that may disqualify the applicant from being eligible for access to classified information. The Government has the burden of establishing controverted facts alleged in the SOR. *See Egan*, 484 U.S. at 531. "Substantial evidence" is "more than a scintilla but less than a preponderance." *See v. Washington Metro. Area Transit Auth.*, 36 F.3d 375, 380 (4th Cir. 1994). The guidelines presume a nexus or rational connection between proven conduct under any of the criteria listed therein and an applicant's security suitability. *See* ISCR Case No. 15-01253 at 3 (App. Bd. Apr. 20, 2016).

Once the Government establishes a disqualifying condition by substantial evidence, the burden shifts to the applicant to rebut, explain, extenuate, or mitigate the facts. Directive ¶ E3.1.15. An applicant has the burden of proving a mitigating condition,

and the burden of disproving it never shifts to the Government. *See* ISCR Case No. 02-31154 at 5 (App. Bd. Sep. 22, 2005).

An applicant "has the ultimate burden of demonstrating that it is clearly consistent with the national interest to grant or continue his security clearance." ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002). "[S]ecurity clearance determinations should err, if they must, on the side of denials." *Egan*, 484 U.S. at 531.

Analysis

Guideline H, Drug Involvement and Substance Misuse

The security concern under this guideline is set out in AG ¶ 24 as follows:

> 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. Controlled substance means any "controlled substance" as defined in 21 U.S.C. 802. Substance misuse is the generic term adopted in this guideline to describe any of the behaviors listed above.

The Government's evidence and Applicant's admissions in his Answer establish the following condition under AG ¶ 25 that could be disqualifying:

> (a) any substance misuse (see above definition).

The guideline in AG ¶ 26 contains four conditions that could mitigate security concerns arising from substance misuse. Two of these mitigating conditions have possible applicability to the facts of this case:

> (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 taken to overcome this 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 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.

AG ¶ 20(a) is only partially established. Applicant's use of an illegal drug happened about two and one-half years ago and was infrequent. Applicant believes that the circumstances under which he took Edibles to relieve pain were highly unusual, which justified his illegal actions. While I have difficulties with the credibility of much of Applicant's testimony and his demeanor at the hearing, I conclude that his drug use is unlikely to recur if he were granted a security clearance.

More significantly, I find the circumstances under which Applicant used Edibles cast doubt on his reliability, trustworthiness, and good judgment. While he was under consideration for a security clearance and was being investigated in connection with his application, he made a deliberate choice to violate federal law when he felt it was justified by his personal circumstances to do so. This judgment and behavior are antithetical to the requirements of a security clearance holder. A person entrusted to safeguard and protect national security matters cannot put his personal interests ahead of his legal obligation to comply with the criminal laws of the United States. As discussed further below, this type of judgment is part of a pattern of decisions made by Applicant in which he chose self-interest over judicious and wise behavior.

AG ¶ 20(b) is established. Applicant has acknowledged his use of Edibles in April and May 2019 and has established a pattern of abstinence. A doctor has prescribed pain medication for Applicant's injured shoulder, and he does not intend to use illegal drugs in the future to self-medicate so that he can sleep. Also, he has provided a signed statement pursuant to AG ¶ 20(b)(3) declaring his intent not to use illegal drugs in the future.

Guideline M, Use of Information Technology

The security concern under this guideline is set out in AG ¶ 39 as follows:

> 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.

The Government's evidence and Applicant's admissions in his Answer potentially establish the following conditions under AG ¶ 40 that could be disqualifying:

> (a) unauthorized entry into any information technology system;
>
> (c) use of any information technology system to gain unauthorized access to another system or to a compartmented area within the same system; and
>
> (e) unauthorized use of any information technology system.

AG ¶ 40(a) and 40(c) are partially established. Applicant claims that he did not successfully enter another person's information technology system. I am not convinced that this claim is credible. As an IT professional working with other IT professionals who were expert in Linux software, Applicant had sufficient resources available to him to learn how to use the Kali Linux software to successfully enter a password protected network. He testified that he only attempted to use the software on one brief occasion. In his December 2015 SCA, he wrote that he has "been learning how to use Kali Linux," which he obtained months earlier. Ultimately, it is not important whether Applicant was successful in his hacking activities or not, the security concerns about his judgment raised by his conduct in seeking to enter private networks remains and is potentially disqualifying.

AG ¶ 40(e) is established. At the hearing, Applicant used vague language to avoid discussing whether his use of his information technology system, consisting of his computer, the Kali Linux software, and the equipment he purchased at DEFCON, was legal. His testimony was inconsistent with his admission in his 2016 Interview that an unauthorized entry into a computer system would be a violation of law. He did, however, acknowledge both in his SCA and in his testimony that his use of his system was not authorized.

The guideline in AG ¶ 41 contains four conditions that could mitigate security concerns arising from the use of information technology. Two of these mitigating conditions have possible applicability to the facts of this case:

> (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; and
>
> (b) the misuse was minor and done solely in the interest of organizational efficiency and effectiveness.

AG ¶ 41(a) is only partially established. A number of years have elapsed since Applicant engaged in this behavior. There was nothing unusual about the circumstances under which he admits he attempted to break into the WiFi networks of computer systems belonging to others, except for the unusual fact that he did this. Applicant may or may not

attempt to repeat this behavior in the future. Given Applicant's disregard for whether his actions were legal and his acknowledgement that his actions were unauthorized, it is entirely possible that he may decide that he wants to explore this technology further at a future date, which raises the primary issue in this case: Applicant's judgment. As with his illegal use of marijuana for his personal interests, he made the same poor judgment buying and using this hacking equipment. He had an excuse for doing so, *i.e.*, to educate himself in the technology, just as he had an excuse to violate a criminal law using Edibles. Overall, Applicant's behavior using the hacking equipment casts doubt on his reliability, trustworthiness, and good judgment.

AG ¶ 41(b) is only partially established. The frequency of Applicant's use of the hacking equipment may have been minor, but the nature of his poor judgment in doing so was hardly minor. Moreover, his actions were not done solely in the interest of organizational efficiency and effectiveness. He admitted in his testimony that he did not work in the security area of his employer's business, and in particular, was not involved in WiFi security.

Whole-Person Analysis

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. In applying the whole-person concept, an 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 and applying the pertinent adjudicative factors in AG ¶ 2(d), specifically:

> (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.

I have incorporated my comments under Guideline H and Guideline M in my whole-person analysis and considered the adjudicative factors in AG ¶ 2(d). Additional comments are warranted. Applicant is a mature, 49-year-old engineer with a responsible position. When he used Edibles to self-medicate, he was not a young person with limited experience in a work environment. He knew that his use of an Edible violated his employer's drug policy and was illegal under Federal law. He exercised very poor judgment at that time. In 2015, he also exercised very poor judgment trying to use technology equipment for an unauthorized, and likely illegal, purpose. His poor judgment even extends back to his days in the Air Force when he was prematurely separated due to his actions. Perhaps most concerning were Applicant's repeated attempts to minimize and recharacterize his actions. I found much of his testimony about important facts in his

case to strain credibility. Similarly, Applicant's demeanor and wordy responses in his attempts to explain his actions and judgment created serious questions about his reliability and trustworthiness.

Overall, the record evidence as described above leaves me with questions and doubts as to Applicant's eligibility and suitability for a security clearance. After weighing the applicable disqualifying and mitigating conditions and evaluating all of the evidence in the context of the whole person, I conclude Applicant has not mitigated the security concerns raised by his drug involvement and misuse of information technology.

Formal Findings

Paragraph 1, Guideline H:	AGAINST APPLICANT
Subparagraph 1.a:	Against Applicant
Subparagraph 1.b:	For Applicant
Paragraph 2, Guideline M:	AGAINST APPLICANT
Subparagraph 2.a	Against Applicant

Conclusion

I conclude that it is not clearly consistent with the national interests of the United States to grant Applicant national security eligibility for a security clearance. Eligibility for access to classified information is denied.

John Bayard Glendon
Administrative Judge