DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 18-02592
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Brian Farrell, Esq., Department Counsel
For Applicant: Troy Nussbaum, Esq.

10/07/2020

_____

Decision

_____

Curry, Marc E., Administrative Judge:

Applicant mitigated the foreign influence security concerns, but failed to mitigate the security concerns generated by his violation of his employer's Internet use policy. Clearance is denied.

Statement of the Case

On August 30, 2019, the Department of Defense Consolidated Adjudications Facility (DOD CAF) issued a Statement of Reasons (SOR) to Applicant, detailing a single allegation under the security concern for Guideline M, misuse of information technology systems, cross-alleged under Guideline E, personal conduct, explaining why it was unable to find it clearly consistent with the national interest to grant security clearance eligibility. The DOD CAF took the action under Executive Order (EO) 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; and DOD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive) and the National Security Adjudicative Guidelines (AG), effective June 8, 2017.

On September 25, 2019, Applicant answered the SOR, admitting the allegation and requesting a hearing. On January 22, 2020, Department Counsel amended the SOR alleging an additional security concern under Guideline B, foreign influence. Applicant responded on February 1, 2020, admitting that allegation.

The case was assigned to me on February 6, 2020. On February 26, 2020, the Defense Office of Hearings and Appeals issued a notice of hearing, scheduling Applicant's case for March 25, 2020. Because of the COVID-19 Pandemic, that hearing was canceled. On July 10, 2020, the court issued a notice rescheduling the case for August 5, 2020. The hearing was held as rescheduled. I received Government Exhibit (GE) 1 and GE 3 through GE 6. I admitted the first six pages of GE 2, and reserved judgment on the admissibility of the remainder of GE 2. I received Applicant Exhibit (AE) A through AE H. I also took administrative notice, at Department Counsel's request, of the facts set forth in six documents marked as Administrative Notice Document (AN) I through AN VI. The transcript (Tr.) was received on August 17, 2020.

Rulings of Procedure and Evidence

Pages seven through ten of GE 2 are part of a document entitled "[Applicant's] Network Activity Investigation, 1/5/2015." Applicant's counsel objected to its admission, arguing that as an unsigned document with no identifying markers such as a company letterhead, it was unauthenticated. I reserved judgment and left the record open through August 26, 2020 to consider any additional evidence or argument regarding the admissibility of GE 2 in its entirety.

Within the time allotted, Department Counsel submitted an additional exhibit, a copy of an e-mail from Applicant's former supervisor, concerning the investigative report, which I marked as GE 7. On August 26, 2012, Applicant's counsel e-mailed me in response to Department Counsel's submission of GE 7 that I incorporated into the record as AE I. He did not object to GE 7, but renewed his objection to the admissibility of GE 2, pages seven through ten. Upon considering the argument of the parties and the additional exhibits, I admitted GE 2 pages seven through ten into the record.

Findings of Fact

Applicant is a 33-year-old single man. He earned an associate's degree in 2009, and a bachelor's degree in 2013. (Tr. 28) For the past 12 years, he has been working in the information technology field. (Tr. 12, 53) Most recently, since 2018, he has been working for a defense contractor as an information technology specialist. (Tr. 48) He currently holds public trust access to sensitive information. (Tr. 66)

Applicant is a native of Cameroon. He has been a naturalized citizen of the United States since 2011. (Tr. 37) He immigrated to the United States when he was 11 years old and spent the remainder of his childhood living with his uncle, a U.S. citizen. (Tr. 32, 43) In addition to raising Applicant after he immigrated to the United States, his uncle helped finance his education. (Tr. 43) When Applicant first moved to the United States, it was very

expensive to make long-distance calls to Cameroon. (Tr. 39) Consequently, Applicant's parents seldom talked to him. Similarly, they did not often travel to the United States to visit him. Applicant did not hear from his parents or see them for nine years after he relocated. (Tr. 39) Ultimately, although Applicant's relationship with his parents is cordial, he has more of a parental relationship with his uncle than his parents. (Tr. 43)

Currently, Applicant's parents have permanent U.S. residence status. (Tr. 43) They moved here in 2017. Later, Applicant's mother returned to Cameroon. She owns a store that sells baby products. (Tr. 40) Typically, Applicant talks to his mother twice per month. Since the pandemic, he has been talking to her daily. (Tr. 43) Applicant's parents remain married. Applicant's mother travels to the United States approximately two to three times per year to visit Applicant and his father. (Answer to Amendment to the SOR, at 2; Tr. 41) Applicant last travelled to Cameroon to visit his mother in 2013. (GE 1 at 38)

When Applicant's father lived in Cameroon, he owned a cleaning business. (Tr. 39) He suffered a massive, debilitating stroke in 2017. (Tr. 40) Partially paralyzed and non-verbal, it is unlikely that he will return to Cameroon.

Applicant has approximately $27,000 invested in retirement accounts. (Tr. 35) He owns no assets in Cameroon. (Tr. 36)

The United States has had diplomatic relations with Cameroon since Cameroon's independence in 1960. (AN I at 1) Cameroon "plays a key role in regional stability and [is] the strongest regional partner in countering terrorism" in the region. (AN I at 1) Cameroon and the United States are closely engaged in issues that address democracy, governance, regional security, environmental protection, health, and economic development. (AN I at 2) Cameroon has struggled to contain terrorism, particularly in its rural, remote region in the north, where Boko Haram is active, borders are porous, and there is a political insurgency. (AN II at 1) Applicant's mother does not live near this area.

In July 2014, Applicant began a job as a help desk administrator. His duties included maintaining the server and monitoring the network for malware. (GE 2 at 7) Applicant's career goal was to earn a promotion to work on cyber-security projects. (GE 2 at 7; Tr. 49) While working at this job, Applicant was working towards earning a cyber-security certification.

On December 19, 2014, Applicant's employer identified suspicious activity on Applicant's computers. Specifically, an analysis of one of Applicant's computers indicated that he attempted to initiate a peer-to-peer connection with a remote host outside of his employer's network. This type of activity was prohibited because of its potential to bypass the employer's security measures. (GE 2 at 7) Further review of Applicant's computer use "discovered attempts to obscure Internet activity by using an anonymous proxy that would hide the destination from [the employer's] IT security systems, as well as frequent visits to questionable download websites as far back as September 2015." (GE 2 at 7) Moreover, Applicant was visiting websites that provided tutorials regarding how to crack passwords and conduct network attacks, and that he had downloaded a copy of pirated software onto

the network. (GE 2 at 9) After an investigation, Applicant was terminated for violation of his employer's Internet use policy. (Answer at 1-2)

Applicant admits that he demonstrated bad judgment accessing some of his "personal stuff" on his work computer. (Tr. 58) However, he contends that he visited hacking-related websites for educational and professional development, and that cyber-security experts need to understand how hackers operate in order to defend against them. (Answer at 2; Tr. 56) He characterized this concept as "ethical hacking," and testified that he was earning an online certification in this field while he was working for his former employer. (Tr. 54) Applicant contends that his employer allowed him to use the office computer for studying and practical assignments related to his certification during down time. Also, Applicant testified that he made a mistake by not memorializing this permission in writing. (Tr. 57-58; 119)

There were occasions on Applicant's job when information technology specialists might need to visit websites related to hacking for research, or download password-cracking software to gain access to a system where a password was lost. These situations were exceedingly rare. (GE 2 at 8) Applicant's employer characterized the volume of hacking-related content combined with the absence of any specific project that required that type of information "disconcerting," and characterized Applicant's behavior as a demonstration of "incredibly poor judgment." (GE 2 at 9) Subsequently, Applicant was terminated from his job.

After Applicant's termination, he completed the certificate in ethical hacking that he had been working on while employed. (Tr. 69) In the past five years, he has completed multiple trainings, including an insider threat training and two cybersecurity awareness trainings. (AE B – AE E) He took these courses to ensure that mistakes such as those which led to his termination in 2015, do not recur. (Answer at 2)

Applicant informed all of his subsequent employers of the circumstances related to the 2015 termination. He is highly respected on the job. According to a coworker, he is "a very trustworthy, hardworking, diligent individual," whose knowledge of cybersecurity and the rules that govern cybersecurity is unparalleled. (AE F)

Policies

The U.S. Supreme Court has recognized the substantial discretion the Executive Branch has in regulating access to information pertaining to national security, emphasizing that "no one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988). When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the adjudicative guidelines. In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially disqualifying conditions and mitigating conditions, which are required to be considered in evaluating an applicant's eligibility for access to classified information. These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, these guidelines are applied together with the factors listed in the adjudicative process. The

administrative judge's overall adjudicative goal is a fair, impartial, and commonsense decision. According to AG ¶ 2(c), the entire process is a conscientious scrutiny of a number of variables known as the "whole-person concept." The administrative judge must consider all available, reliable information about the person, past and present, favorable and unfavorable, in making a decision.

The protection of the national security is the paramount consideration. AG ¶ 2(b) requires that "[a]ny doubt concerning personnel being considered for national security eligibility will be resolved in favor of the national security." In reaching this decision, I have drawn only those conclusions that are reasonable, logical, and based on the evidence contained in the record. Under Directive ¶ E3.1.14, the Government must present evidence to establish controverted facts alleged in the SOR. Under Directive ¶ E3.1.15, the applicant is responsible for presenting "witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by applicant or proven by Department Counsel. . . ." The applicant has the ultimate burden of persuasion to obtain a favorable security decision.

A person who seeks access to classified information enters into a fiduciary relationship with the Government predicated upon trust and confidence. This relationship transcends normal duty hours and endures throughout off-duty hours. The Government reposes a high degree of trust and confidence in individuals to whom it grants access to classified information. Decisions include, by necessity, consideration of the possible risk that the applicant may deliberately or inadvertently fail to safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation about potential, rather than actual, risk of compromise of classified information. Section 7 of Executive Order 10865 provides that decisions shall be "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." *See also* EO 12968, Section 3.1(b) (listing multiple prerequisites for access to classified or sensitive information).

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

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

Analysis

Guideline B: Foreign Influence

The security concern under Guideline B is set forth in AG ¶ 6, as follows:

> Foreign contacts and interests, including, but not limited to, business, financial, and property interests, are a national security concern if they result in divided allegiance. They may also be a national security concern if they create circumstances in which the individual may be manipulated or induced to help a foreign person, group, organization, or government in a way inconsistent with U.S. interests or otherwise made vulnerable to pressure or coercion by any foreign interest.

Cameroon is an ally of the United States and there is no record evidence that Cameroon is engaging in espionage against the United States. However, Cameroon has experienced difficulties with terrorism and political instability. Under these circumstances, Applicant's relationship to his mother, a citizen and resident of Cameroon, triggers the application of AG ¶ 7(a) "contact, regardless of method, with a foreign family member, business or professional associate, friend, or other person who is a citizen of or resident in a foreign country if that contact creates a heightened risk of foreign exploitation, inducement, manipulation, pressure, or coercion."

The politically unstable part of Cameroon where terrorism is prevalent is a rural area that is far from where Applicant's mother lives. Moreover, Applicant has spent nearly his entire life in the United States, immigrating here when he was 11 years old to live with his uncle. Applicant was educated in the United States, and all of his assets are here. Under these circumstances, AG ¶ 8(b), "there is no conflict of interest, either because the individual's sense of loyalty or obligation to the foreign person, or allegiance to the group, government, or country is so minimal, or the individual has such deep and longstanding relationships and loyalties in the United States, that the individual can be expected to resolve any conflict of interest in favor of the U.S. interest," applies. I conclude Applicant has mitigated the foreign influence security concern.

Guideline M, Use of Information Technology

The security concerns generated by this guideline are set forth in AG ¶ 39, as follows:

> Failure to comply with rules, procedures, guidelines, or regulations pertaining to information technology systems may raise concerns about an individual's reliability and trustworthiness, calling into question the willingness or ability to properly protect sensitive systems, notebooks, and information. Information technology includes . . . any component, whether integrated into a larger system or not, such as hardware, software, or firmware, used to facilitate these transactions.

Applicant's multiple violations of his employer's Internet use policy triggers the application of the following disqualifying conditions under AG ¶ 40:

> (e) unauthorized use of any information technology system; and
>
> (f) introduction . . . of hardware, firmware, software, or media to or from any information technology system when prohibited by rules, procedures, guidelines, or regulations, or when otherwise not authorized.

Applicant has had no additional episodes of misuse of information technology for more than five years. He has informed all of his subsequent employers of the details regarding his termination, completed multiple trainings, and is highly respected on his current job. These favorable facts raise the issue of whether the mitigating condition set forth in AG ¶ 41(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," applies.

Applicant contends that he had permission to visit hacking-related websites, and was accessing them either as part of his job, or in an effort to further his cyber-security studies. This contention raises the issue of whether the mitigating condition set forth in AG ¶ 41(d), "the misuse was due to . . . unclear instruction," applies.

Applicant's violations of his ex-employer's Internet use policy were extremely serious, as they involved visiting websites containing network hacking and password-cracking tutorials. These violations were particularly egregious because Applicant was responsible, in part, with developing malware defenses for his employer. Under these circumstances, his behavior continues to cast doubt on his reliability, trustworthiness, and good judgment, and AG ¶ 41(a) is inapplicable. Given the unusually high volume of visits to inappropriate hacking websites, and in light of evidence that Applicant attempted to obscure some of his illicit Internet activity, AG ¶ 41(d) also does not apply. Efforts to conceal his conduct show consciousness of guilt, that is, he was aware that his Internet activity was not permitted. In sum, there is limited evidence of mitigation, but in light of the nature and seriousness of the violations, it is insufficient to fully mitigate the security concerns.

Guideline E, Personal Conduct

Under this guideline, "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." (AG ¶ 15) Since Guideline E concerns only a cross-allegation, security concerns under Guideline E are essentially duplicative and separate analysis is unnecessary. Applicant's conduct is nevertheless disqualifying and unmitigated under this guideline for the same reasons as discussed above under Guideline M.

Whole-Person Concept

I considered the whole-person factors in my consideration of the disqualifying and mitigating conditions set forth under Guidelines B, M, and E. They do not warrant a favorable conclusion.

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 M:	AGAINST APPLICANT
Subparagraph 1.a:	Against Applicant
Paragraph 2, Guideline E:	AGAINST APPLICANT
Subparagraph 2.a:	Against Applicant
Paragraph 3, Guideline B	FOR APPLICANT
Subparagraph 3.a:	For Applicant

Conclusion

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

_____
Marc E. Curry
Administrative Judge