DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 23-01737
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Adrienne M. Driskill, Esq., Department Counsel
For Applicant: Jason S. Ayeroff, Esq.

10/30/2024

_____

Decision

_____

OLMOS, Bryan J., Administrative Judge:

Applicant mitigated the security concerns under Guideline K (Handling Protected Information), Guideline M (Use of Information Technology), and Guideline E (Personal Conduct). Eligibility for access to classified information is granted.

Statement of the Case

Applicant submitted a security clearance application (SCA) on November 17, 2022. On September 26, 2023, the Department of Defense (DOD) issued a Statement of Reasons (SOR) to Applicant detailing security concerns under Guideline K, Guideline M, and Guideline E. The DOD issued the SOR under Executive Order (Exec. Or.) 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 Security Executive Agent Directive 4 (SEAD 4), *National Security Adjudicative Guidelines* (AG), effective June 8, 2017.

Applicant answered the SOR on June 21, 2023 (Answer), and initially requested a decision based on the administrative written record. Subsequently, Applicant requested a hearing before an administrative judge from the Defense Office of Hearings and Appeals (DOHA). The case was assigned to me on August 22, 2024. On August 27, 2024, DOHA issued a notice scheduling the hearing for September 27, 2024.

I convened the hearing as scheduled. Department Counsel offered into evidence Government Exhibits (GX) 1-2. Applicant testified and offered into evidence Applicant Exhibits (AX) A-I. All exhibits were admitted without objection. Additionally, two witnesses testified on Applicant's behalf. The record closed at the conclusion of the hearing. DOHA received the hearing transcript (Tr.) on October 7, 2024.

Findings of Fact

In his Answer to the SOR, Applicant admitted all of the SOR allegations and provided explanations. His admissions are incorporated into my findings of fact. After a thorough and careful review of the pleadings and evidence submitted, I make the following additional findings of fact.

Applicant is 25 years old. He grew up in a small community and used his athletic abilities to leave home at the age of 15 to play basketball for a large high school in another state. He was then awarded a scholarship and attended a private high school in a third state where he played his senior year. While his hopes for a NCAA Division I athletic scholarship did not materialize, he was able to attend a college near his private high school and earned a bachelor's degree in mechanical engineering in 2022. He started with his current, sponsoring employer in January 2023. (GX 1-2; AX G; Tr. 61-68)

SOR ¶¶ 1(a), 2(a) and 3(a) involve a single incident in June 2021, when Applicant violated security protocols, specific to Company A, by removing a laptop that contained sensitive information from an unclassified but secured area and accessing that laptop without authorization. He admitted the allegations and detailed that, in the summer prior to his senior year in college, he worked as an intern with Company A, a large web-based services corporation. His duties were to maintain several technical aspects of the data center in his building which included a secured area where sensitive client information was housed on various computers and laptops. This secured area was manned by a guard who would use a hand-held metal detector to verify that individuals did not enter the area with any outside electronics. There were times, particularly early in the morning, when no guard was present. Applicant accessed this area regularly as part of his internship duties. (GX1-2; Tr. 71-80, 100-104)

As part of his job, Applicant was assigned a portable laptop that he could take to and from the office. One Friday morning, about three weeks into the internship, he forgot his laptop at home. Rather than return home to get the laptop or notify his supervisor, he took a laptop from the secured area to use for the day. These secured laptops were physically identical to his assigned laptop. He worked his normal shift and engaged with

colleagues without incident. He testified that he used the secured laptop to access information and systems within the company like he would have with his assigned laptop and did not access, download, or manipulate any sensitive information contained on the secured laptop. However, in a rush to start his weekend, he placed the laptop unsecured in his desk at the end of the day and returned it to the secured area early that following Monday when no security guard was present. (GX 1-2; Tr. 85-105)

Later on that Monday, Applicant was confronted by security personal about the incident. Following a meeting with human resources in which he admitted his actions, his internship was terminated. Applicant testified that, at the time, he was unaware that he had violated company policies by removing and using a laptop from the secured area. However, he also admitted that he did not pay attention to all aspects of his training as he was excited to get started with Company A. In retrospect, he acknowledged that he should have communicated with his supervisor and sought more guidance and clarification over the entire situation. He described feeling "shame" over the incident. (Answer; GX 1-2; Tr. 85-105)

Applicant detailed that he has used lessons learned from the laptop incident in his current employment. In early 2023, after receiving an interim security clearance, he conducted research that required accessing both open-source and classified information. He described reviewing security procedures within his current work and seeking guidance from his supervisor and a security officer on the procedures for using an unclassified computer in a secured area. (Tr. 115-122)

SOR ¶ 3(c) alleges that, on various occasions in 2022, Applicant deliberately falsified job applications by claiming to have security clearances that he did not possess. He admitted the allegation and stated that, during his senior year of college, he applied for several hundred job postings, primarily with Company B, a government contractor. He would review Company B's online job postings and submit electronic applications to multiple positions at a time. However, he grew frustrated at the lack of responses he received from recruiters and worried that he would soon graduate from college without a job. Therefore, he began to apply for positions that were beyond his qualifications or that required a security clearance. Even though he did not hold a security clearance, he believed that applying to these positions and affirmatively checking application boxes indicating that he held a security clearance would help get his application reviewed by recruiters. He testified that he submitted an accurate resume with his applications and hoped that, once a recruiter saw his application, he would be interviewed for a position appropriate to his skill set. (Answer; GX 2; Tr. 80-85, 109-120)

Ultimately, Applicant was contacted by a representative of Company B and told to stop submitting applications to positions for which he did not qualify. Immediately following that notification, Applicant stopped submitting applications for positions that were beyond his qualifications and stopped indicating that he held a security clearance. He volunteered details of this event during his investigation. He later testified that he

displayed poor judgment in submitting applications that were not accurate to his circumstances and that his actions were a mistake. (Tr. 112-120)

Lastly, SOR ¶ 3(b) alleges that Applicant falsified his November 2022 SCA by failing to disclose prior marijuana use. He admitted the allegation and stated that, on one occasion over a winter break in college, he consumed a brownie containing marijuana with friends. He admitted he did not disclose his drug use in his SCA because he felt embarrassment and shame over his actions. However, he voluntarily disclosed his drug use in his January 2023 background interview with a DOD investigator. During the interview, in his answer to the SOR and in his testimony, he admitted he was wrong not to initially disclose his drug use. He testified that he understood the importance of providing accurate information in all aspects of his employment and that he had an ongoing obligation to disclose information that may be unfavorable, but relevant to holding a security clearance. He further stated that he tried marijuana only on the one occasion and understood that any illegal drug use is in conflict to holding a security clearance. (Answer; GX 1-2; Tr. 88-95)

Applicant stated that he was young and lacked experience in much of his decision making. He acknowledged that he would benefit from mentorship and career guidance. He testified that he would communicate with his leadership and research mentorship options through his current employer. (Tr. 87-90, 120-126)

Ms. K testified on Applicant's behalf. She was also an intern at Company A in 2021 and worked in an adjacent building to Applicant. She could not recall any specific training that she or Applicant received regarding accessing or removing laptops from the secured area. However, she believed it was generally known that the area was restricted and that removal of equipment from the area was prohibited. She testified that Applicant had felt remorse and regret over the situation at Company A, had matured over the years, and was trustworthy. (Tr. 24-39)

Ms. C also testified on Applicant's behalf and is his half-sister. She described that Applicant initially had difficulty transitioning away from home during his teenage years but had matured as he completed college and entered his career. He lived with her and her family for several months in 2022 and 2023. She described him as trustworthy and engaging with her children. (Tr. 48-57)

Applicant also submitted several character letters from individuals who have known him over the years. His current supervisor stated that he interacted with Applicant daily and found him to be diligent and responsible. He noted that Applicant also took an active approach to maintaining security procedures. Two of Applicant's former professors stated that he adhered to laboratory protocols while at the university and was a reliable, compassionate, and trustworthy individual who took his responsibilities seriously. Lastly, a former coach stated that Applicant was always respectful and focused. (AX A-D)

Policies

It is well established that no one has a right to a security clearance. As the Supreme Court held in *Department of the Navy v. Egan*, "the clearly consistent standard indicates that security determinations should err, if they must, on the side of denials." 484 U.S. 518, 531 (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 used in evaluating an applicant's eligibility for access to classified information.

These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, these guidelines are applied in conjunction with the factors listed in the adjudicative process. The administrative judge's overarching adjudicative goal is a fair, impartial, and commonsense decision. According to AG ¶ 2(a), the entire process is a 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. 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 classified information. Such decisions entail a certain degree of legally permissible extrapolation of potential, rather than actual, risk of compromise of classified information.

Analysis

Guideline K: Handling Protected Information and Guideline M: Use of Information Technology

AG ¶ 33 articulates the Government's security concern about handling protected information:

> Deliberate or negligent failure to comply with rules and regulations for handling protected information-which includes classified and other sensitive government information, and proprietary information-raises doubt about an individual's trustworthiness, judgment, reliability, or willingness and ability to safeguard such information, and is a serious security concern.

I have considered the disqualifying conditions for the handling of protected information under AG ¶ 34 and the following are potentially applicable:

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

AG ¶ 39 articulates the Government's security concern about the use of information technology:

> 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.

I have considered the disqualifying conditions for the use of information technology under AG ¶ 40 and the following is potentially applicable:

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

Guideline K security concerns are not limited to violations of DOD rules and polices, but also encompass violations of industry rules and policies established for the protection of classified and sensitive information. *See* ISCR Case No. 15-08002 at 1 (App. Bd. July 17, 2018); ISCR Case No. 14-00963 at 3 (App. Bd. Jan. 13, 2015). Disqualifying

conditions under Guideline K and Guideline M do not require an actual compromise of protected information or proof of actual misuse or subsequent transmission of the protected information. *See* ISCR Case No. 20-00230 at 3 (App. Bd. Dec. 10, 2021).

Record evidence and testimony establish that Applicant entered a secured area of Company A in June 2021 and, without authorization, removed a laptop that contained sensitive information. He proceeded to access Company A's systems from that laptop but did not access any secured information. Still, he then left the laptop unsecured in his workspace over the weekend. His internship was terminated due to his violation of company policies. At the time, Applicant was unaware that his actions were against company policy. However, he acknowledged that he should have paid greater attention to the initial training he received. Regardless of his intent, his unauthorized removal of the laptop, subsequent use of systems on the laptop and eventual storage of the laptop in an unauthorized location establish the disqualifying conditions for SOR ¶ 1.a under AG ¶¶ 34(b) and 34(g) and SOR ¶ 2.a under AG ¶ 40(e).

I have considered the mitigating conditions for the handling of protected information under AG ¶ 35 and the following is potentially applicable:

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

I have considered the mitigating conditions for the use of information technology under AG ¶ 41 and the following is 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;

Applicant candidly recognized that he made a poor decision in taking a laptop out of the secured area in Company A without authorization, using it for the day, and leaving it unsecured in his work area over the weekend. He also recognized that he should have asked his manager for assistance or sought clarification from his security personal before taking the laptop.

In the three years following the termination of his internship with Company A, Applicant has become more attentive to security procedures and company policies. He demonstrated this increased awareness at his current job by asking for clarification of security procedures before moving an unsecured laptop in and out of a classified area. His supervisor described him as diligent and responsible. I believe Applicant has learned from his mistake and his unauthorized access and mishandling of sensitive information is unlikely to recur. He is committed to following the rules and procedures of his workplace and communicating with his management and security personnel when clarification is

needed. Mitigation under AG ¶ 35(a) applies to SOR ¶ 1.a. Mitigation under AG ¶ 41(a) applies to SOR ¶ 2.a.

Guideline E: Personal Conduct

AG ¶ 15 articulates the Government's security concern about 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 or sensitive information. Of special interest is any failure to cooperate or provide truthful and candid answers during national security investigative or adjudicative processes.

I have considered the disqualifying conditions for personal conduct under AG ¶ 16 and the following are 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 national security eligibility or trustworthiness, or award fiduciary responsibilities;
>
> (b) deliberately providing false or misleading information; or concealing or omitting information, concerning relevant facts to an employer, investigator, security official, competent medical or mental health professional involved in making a recommendation relevant to a national security eligibility determination, or other official government representative; and
>
> (c) credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any other single guideline, but which, when considered as a whole, supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the individual may not properly safeguard classified or sensitive information.

An applicant who deliberately fails to give full, frank, and candid answers to the Government in connection with a security clearance investigation interferes with the integrity of the industrial security program. ISCR Case No. 01-03132 (App. Bd. Aug. 8, 2002) The Government must produce substantial evidence that an omission was deliberate and not merely that the omission occurred. ISCR Case No. 07-16511 (App. Bd. Dec. 4, 2009)

SOR ¶ 3.a is a cross-allegation of the security concerns related to the handling of protected information. Applicant's failure to comply with rules and regulations regarding the handling of protected information while working with Company A is discussed under Guideline K above. However, his failure to seek guidance from his leadership or promptly return the laptop at the end of the workday raise sufficient whole-person concerns for AG ¶ 16(c) to be applicable.

Applicant also provided false information in multiple job applications by falsely stating that he possessed a security clearance. He then failed to disclose his marijuana use in his November 2022 SCA. Security concerns under AG ¶ 16(a) are applicable to SOR ¶ 3.b. Security concerns under AG ¶ 16(b) are applicable to SOR ¶ 3.c.

I have considered the mitigating conditions for personal conduct under AG ¶ 17 and the following is potentially applicable:

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

Applicant's removal and use of a secured laptop in June 2021 was not a minor breach of company procedures, as it led to the termination of his internship. However, it occurred under unique circumstances, and he took action to not repeat that mistake by focusing on security rules and procedures within his current employment and reaching out to management and security personal for clarification as needed. This event no longer casts doubt on Applicant's reliability, trustworthiness or judgment. Mitigation under AG ¶¶ 17(c) and 17(d) apply to SOR ¶ 3.a.

Applicant's repeated submission of job applications in 2022 that contained false information was also not a minor offense. Applicant claimed that, at the time, he was only trying to get a recruiter to look at his resume, which was accurate and attached to the electronic application. However, he acknowledged that this was a significant lapse of judgment on his part and volunteered details of his actions during his background investigation. This action has not been repeated and no longer casts doubt on Applicant's reliability, trustworthiness, or judgment. Mitigation under AG ¶¶ 17(c) and 17(d) apply to SOR ¶ 3.c.

Applicant also deliberately failed to disclose any drug use in his November 2022 SCA. He then voluntarily disclosed his drug use during his background interview with an investigator in January 2023. At hearing, he candidly provided details of his drug use and admitted that he did not initially disclose that use out of shame and embarrassment. However, he testified that he has come to understand the importance of providing accurate information in all aspects of his employment and that he has an ongoing obligation to disclose information that may be unfavorable, but relevant to holding a security clearance. He voluntarily corrected the omission prior to being confronted and understood the significance of his actions. Mitigation under AG ¶¶ 17(a) and 17(d) apply to SOR ¶ 3.b.

Whole-Person Concept

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

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

Under AG ¶ 2(c), the ultimate determination of whether to grant eligibility for a security clearance must be an overall commonsense judgment based upon careful consideration of the guidelines and the whole-person concept.

I considered the potentially disqualifying and mitigating conditions in light of all the facts and circumstances surrounding this case. I have incorporated my comments under Guideline K, Guideline M and Guideline E in my whole-person analysis.

In reviewing the allegations as a whole, Applicant made a series of decisions towards the end of college and at the start of his professional career that reflected poorly on his judgment, reliability and trustworthiness. However, he acknowledged his mistakes and articulated changes that he made over time to become a trustworthy and reliable young professional. He also recognized that he would benefit from greater career guidance and mentorship and committed to researching support through his current employer.

I had the opportunity to observe Applicant's demeanor during his testimony and found that he was credible and candid. I believe he has learned from his mistakes and

will not repeat them. He now has a better understanding of the rules and regulations that govern the protection of classified and sensitive information, including the need for total candor in the security clearance process. Overall, the record evidence leaves me without questions or doubts about Applicant's eligibility and suitability for a security clearance. I conclude Applicant mitigated the security concerns.

Formal Findings

Formal findings for or against Applicant on the allegations set forth in the SOR, as required by section E3.1.25 of Enclosure 3 of the Directive, are:

Paragraph 1, Guideline K:	FOR APPLICANT
Subparagraph 1.a:	For Applicant
Paragraph 2, Guideline M:	FOR APPLICANT
Subparagraph 2.a:	For Applicant
Paragraph 3, Guideline E:	FOR APPLICANT
Subparagraphs 3.a-3.c:	For Applicant

Conclusion

In light of all of the circumstances, it is clearly consistent with the national interest to grant Applicant a security clearance. Eligibility for access to classified information is granted.

_____
Bryan J. Olmos
Administrative Judge