DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 23-00944
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Sakeena Farhath, Esq., Department Counsel
For Applicant: *Pro se*

06/05/2024

Decision

OLMOS, Bryan J., Administrative Judge:

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

Statement of the Case

Applicant submitted a security clearance application (SCA) on August 18, 2020. On July 19, 2023, the Department of Defense (DOD) issued a Statement of Reasons (SOR) to Applicant detailing security concerns under Guideline M, Guideline K 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 August 8, 2023, and requested a hearing before an administrative judge from the Defense Office of Hearings and Appeals (DOHA). The case was assigned to me on November 6, 2023. On January 29, 2024, DOHA issued a notice scheduling the hearing for February 22, 2024.

I convened the hearing as scheduled. Department Counsel offered into evidence Government Exhibits (GX) 1-4. Applicant testified and offered into evidence Applicant Exhibits (AX) A-O. All exhibits were admitted without objection. Two witnesses also testified and provided character evidence on behalf of Applicant. I held the record open through March 8, 2024, to allow both parties the opportunity to submit additional documents. Applicant submitted an additional exhibit, AX P, which was admitted without objection. DOHA received the hearing transcript (Tr.) on February 29, 2024. The record closed on March 8, 2024.

Findings of Fact

In his Answer to the SOR, Applicant admitted all of the allegations with 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 39 years old. He is married and has two children. He completed a bachelor's degree in 2014 with a focus in business administration. He has worked for his current employer since February 2018 and is a manager of engineering operations. He does not hold a security clearance. (GX 1; Tr. 20-21)

In about November 2016, Applicant traveled to the location of another U.S. Government Agency (OGA) to undergo a polygraph interview for a security clearance. During the interview, he realized that he had a firearm in his vehicle which was in violation of federal law. He informed the investigators and was escorted by security to his vehicle where he surrendered the firearm. He was subsequently charged with a firearms offense. (GX 1-2, GX 4; Tr. 75-77)

Applicant stated that he maintained a "concealed carry" permit and forgot that he had the firearm in his vehicle when he drove onto Government property. Following the completion of 20 hours of community service, the charges were dismissed. Applicant stated that, since the arrest, he allowed his "concealed carry" permit to expire and he no longer carries a firearm in his vehicle. (GX 4; Tr. 75-77)

In March 2017 and again in October 2018, Applicant was denied a security clearance by the OGA. As part of those OGA investigations, he participated in multiple polygraph interviews and disclosed a history of activities that serve as the basis for the Government's current security concerns. In August 2020, he submitted an SCA to DOD and listed that he had been denied a security clearance by the OGA for concerns over "personal conduct and use of information systems." He also detailed that, as a systems administrator, he had previously “access[ed] employee records without explicit authorization.” (GX 1-2; Tr. 100-105, 118-120)

While the DOD investigation was ongoing, Applicant submitted another application for access to classified information to the OGA, which was denied in September 2022. This OGA application and initial denial are not part of the record evidence. He appealed the OGA decision. In February 2023, he received a letter from an OGA senior appeals officer affirming the denial. This letter is part of the record evidence as GX 2. It provides a summary of Applicant’s past conduct that resulted in OGA’s denial of his application. This conduct was also alleged in the SOR. (GX 2; Tr. 74-82)

The OGA denial letter summarized several concerns, including that, over an unspecified period of time, Applicant had illegally downloaded movies, songs, games, and books with an estimated value of $23,000. In his June 2023 response to DOD interrogatories, Applicant admitted that he illegally downloaded media and software through about 2011. He testified that he knew that the illegal downloading was wrong and he stopped because he did not want it to interfere with his ability to obtain work in cyber-related security. (GX 2, GX 4; Tr. 110-113)

The OGA denial letter further stated that Applicant disclosed that he had a pornography addiction and had previously streamed pornographic images on his work computer. In his June 2023 interrogatory response, Applicant stated he only recalled looking at pornography while working for a company in 2003 when he was still in high school. (GX 2, GX 4)

However, in his Answer and in his testimony, Applicant stated that he also viewed pornography from a work computer while with Employer A, but could not recall the frequency of his viewing. He worked with Employer A from about August 2008 through October 2011 and described the company as a small healthcare management practice run by just one other person. (Answer; Tr. 86-95, 115-116)

The OGA denial letter also stated that, between 2008 and 2011, Applicant “accessed patients’ personal and medical files out of boredom and curiosity, to include medical information on a patient who [he] knew” and that he continued to access medical and personal files between 2011 and 2013. (GX 2) (SOR ¶ 2.b) Applicant explained that, as part of this job, he would go into medical practices and assist them in transitioning from paper to electronic medical records. He testified only remembering one occasion, in 2009, that he viewed patient medical records. At the time, while tasked to learn about the medical records management system one of his clients was utilizing, he recognized a patient’s name on his client’s appointments calendar. The patient was one of Applicant’s former high school classmates. He opened and viewed the patient’s medical records as well as the purpose for the upcoming visit. He testified that he knew at the time that the information was protected, but he did not give his actions any significant thought. He claimed he did not further disseminate the information and that Employer A never knew of his actions. (Answer; GX 2, GX 4; Tr. 86-103)

Although the OGA denial letter stated that Applicant reviewed medical records on multiple occasions from 2008 through 2013, he claimed to only remember the one occasion in 2009 and believed the denial letter was not "100 percent accurate." (Tr. 105) Additionally, he worked with Employer B from October 2011 through October 2013. In that position, he built websites and marketing material for clients and claimed not to have access to medical records or personal identifying information (PII). (Answer; GX 2, GX 4; Tr. 104-108)

Applicant began working with Employer C in about October 2014. The OGA denial letter stated that, while employed as a system administrator with Employer C from 2015 through 2016, Applicant accessed human resource files to view the addresses of about 70 employees to "see what houses the employees could afford." (GX 2) Applicant later accessed a document "containing manager and supervisor salaries, bonuses, and social security numbers." (GX 2-4; Tr. 85-90) (SOR ¶ 2.a)

In his SCA, Applicant stated that, while working with Employer C, he "accessed employee records without explicit authorization" and "abused" the trust of the company he was working for at the time. (GX 1) He detailed that, as a system administrator, he was responsible for "managing the communications systems, networks and server infrastructure" for his company. (GX 3) On multiple occasions in that position, he accessed a human resources spreadsheet that contained PII for everyone in the company. This included employee birthdates, salaries, spousal names and mailing addresses. He stated he accessed the files because he was "curious about where [his] coworkers lived, what their salaries were and how much their houses cost." (GX 3) He claimed he last viewed those records in early 2016 and did not disseminate the information. (Answer; GX 1, GX 3; Tr. 110-120)

Applicant further stated that, at the time of the incident, he did not consider reporting it to Employer C as he "did not perceive it as an issue." (GX 3) With regard to both Employer A and Employer C, he stated he recognized that he worked in a "position of trust" but claimed that he had "no formal training and guidance on how to handle sensitive information and or PII." (Answer) He stated he was "young, inexperienced, and did not know any better" at the time. (Answer; Tr. 102-115)

Applicant left Employer C for Employer D, his current employer, in about February 2018. He claimed since "surrounding myself with information privacy and security focused individuals, I now realize how wrong I was in accessing that information without direct and explicit consent." (GX 3) He claimed while with Employer D, he received proper training on how to handle sensitive information and "finally had clearly defined rules to abide by." (Answer) He is now considered a "respected leader" with Employer D and is "tasked with enforcing and implementing new policy, controlling and managing access to enclaves and sensitive systems, and educating [Employer D's] workforce." (Answer) He stated his intent to not repeat his past mistakes. (Answer; GX 3-4; Tr. 23-27)

Applicant also described working with an individual therapist since June 2022. The therapist submitted a letter stating Applicant had discussed the past clearance incidents and had been "accountable and acknowledged that [his] behavior was not only inappropriate but also a detriment to his character at the time." (AX H) She further noted that Applicant had shown "personal and professional growth" over time. (AX H) Similarly, Applicant was seeing a performance psychology coach sponsored by Employer D. This performance coach stated Applicant had undergone "self-reflection" over his past actions and was working to be a better leader in the workplace. (Answer; AX G-H; Tr. 24-28, 84-85)

Two witnesses testified on Applicant's behalf at his hearing. Mr. H is a vice president with Employer D and currently holds a security clearance. He has known Applicant for nearly four years and is his direct supervisor. Mr. H testified that Applicant had not experienced any security incidents while with Employer D and was highly protective of company policies and procedures. Mr. H also testified that Applicant was committed to maintaining the security environment of the workplace and was a trusted team leader in the office. (AX C; Tr. 40-54)

Mr. P is the Chief Information Officer at Employer D, currently holds a security clearance and has also known Applicant for nearly four years. Mr. P testified that Employer D focuses on various aspects of cyber security and is particularly attuned to cyber and insider threats. From that perspective, he testified that he was aware of Applicant's past transgressions but believed that Applicant had "worked to rehabilitate his character." Mr. P also stated that Applicant actively participates in security training and is a highly valued member of the company. (AX A; Tr. 54-72)

Applicant also submitted character reference letters, primarily from colleagues within Employer D. Several character references spoke to Applicant's maturation, particularly since starting with Employer D in 2018 and his individual efforts to improve security procedures on the job. They found Applicant to have shown "exemplary professional conduct" with a "composed demeanor." (AX D-E) Annual performance reviews from the last three years reflect that he has performed at or above expectations and met all of his training requirements. (AX B, AX F, AX L, AX P)

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 M, Use of Information Technology

The security concern relating to this guideline 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.

The adjudicative guideline notes several conditions that could raise security concerns under AG ¶ 40. The following are potentially applicable in this case:

(a) unauthorized entry into any information technology system; and

(e) unauthorized use of any information technology system.

From about August 2008 through October 2011, while working with Employer A, Applicant accessed and reviewed patient medical records on multiple occasions and without authorization. He did not have access to PII while with Employer B from October 2011 through October 2013. However, from about 2015 through early 2016, he accessed human resource files at Employer C without authorization. This information included salaries, home addresses and social security numbers of employees and management. While with Employer A and Employer C, he breached the trust of his employers and the privacy of several individuals. Disqualifying conditions AG ¶¶ 40(a) and 40(e) apply.

AG ¶ 41 describes potentially applicable mitigating conditions for the misuse of information technology including:

(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.

Several years have passed since Applicant accessed medical records and human resource records without authorization. Additionally, he has been working with Employer D since 2018 and claims to have benefited from the higher security standards and training of that company. Therefore, AG ¶ 41(a) has some application.

Nonetheless, Applicant breached the trust of his employers and the privacy of many individuals on multiple occasions from 2008 through 2011 and again from 2015 through early 2016. These actions were entirely unrelated to the requirements of his positions.

At the time of his unauthorized viewing of Employer C's records, Applicant was a system administrator and was responsible for managing the communication systems, networks and server infrastructure for his company. Yet, at the time of the unauthorized access, Applicant stated he did not perceive his actions to be an issue and claimed that he did not have proper training on how to handle sensitive information. This apparent lack of training does not excuse his actions nor mitigate the security concerns. He was aware that his actions were wrong, but proceeded to commit a substantial breach of privacy anyway.

Applicant also never disclosed his actions to either Employer A or Employer C. Instead, he first provided details of his actions only while undergoing an OGA investigation with polygraph examination. His lack of disclosure to either employer at the time of the incidents undercuts mitigation and raises questions of judgment and trustworthiness.

Additionally, Applicant illegally downloaded media and software and viewed pornography on his work computer through 2011. This additional information was not alleged under Guideline M in the SOR, so it cannot be considered as disqualifying conduct. However, in weighing mitigation, it shows that Applicant's improper use of information technology was not an isolated event or occurred under unusual circumstances. Instead, it demonstrates a pattern of rule violations. Applicant has not met his burden of establishing mitigation under AG ¶ 41(a).

Guideline K, Handling Protected Information

The security concern relating to the guideline for handling protected information is set out in AG ¶ 33:

> 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.

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).

AG ¶ 34 describes conditions that could raise a security concern and may be disqualifying. I have considered all of them, and the following is potentially applicable:

> (d) inappropriate efforts to obtain or view protected information outside one's need to know.

The Guideline M security concerns are cross-alleged under Guideline K. Applicant's unauthorized access to patient medical records from 2009 through 2011 while with Employer A, and his unauthorized access of human resource information, which was proprietary to Employer C, are sufficient to establish disqualifying condition AG ¶ 34(d).

AG ¶ 35 describes conditions that could mitigate the security concerns and are potentially applicable, including the following:

> (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.

Similar to the reasoning under Guideline M, mitigation of the Guideline K security concerns are not fully applicable under AG ¶ 35(a). On multiple occasions during two separate periods of time, Applicant breached the trust of employers and the privacy of several individuals by accessing medical records, social security numbers, salaries, and other proprietary and personal identifying information.

Particularly as a system administrator for Employer C, Applicant was trusted to safeguard information. Instead, he used his position to feed his personal curiosities. He never informed either employer or any of the individuals of his actions, instead only disclosing the information during a security investigation and polygraph examination. Applicant has not met his burden to establish that these events occurred under unusual circumstances or no longer cast doubt as to his reliability, trustworthiness, or judgment.

Guideline E, Personal Conduct

The security concern relating to this guideline is set out in AG ¶ 15:

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

Under Guideline E, the Government alleges that Applicant was denied a clearance by an OGA in March 2017 and October 2018 for reasons including personal conduct issues, misuse of information systems and a firearms offense. The OGA security clearance decision is informative, but not binding in DOHA proceedings. However, the underlying conduct alleged remains relevant to this assessment of Applicant’s security worthiness.

I have considered the disqualifying conditions for personal conduct under AG ¶ 16 and the following is potentially applicable:

(d) credible adverse information that is not explicitly covered under any other guideline and may not be sufficient by itself for an adverse determination, but which, when combined with all available information, 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. This includes, but is not limited to, consideration of: (1) untrustworthy or unreliable behavior to include breach of client confidentiality, release of proprietary information, unauthorized release of sensitive corporate or government protected information; (2) any disruptive, violent, or other inappropriate behavior; (3) a pattern of dishonesty or rule violations; and (4) evidence of significant misuse of Government or other employer's time or resources.

Applicant's unauthorized access of medical and human resource files while working with two separate employers, along with his firearms offense in 2016 are sufficient whole-person concerns for AG ¶ 16(d) to be applicable. The general security concern under AG ¶ 15 also applies.

Conditions that could mitigate the personal conduct security concerns are provided under AG ¶ 17 and the following are potentially applicable:

(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 carrying of a firearm in his vehicle onto Government property was inadvertent and regrettable. However, he disclosed his error on the day that it occurred and accepted the consequences of his actions. He has since made changes by removing the firearm from the vehicle so that the event would not be repeated. This component of the SOR allegation is mitigated by AG ¶ 17(c).

Still, Applicant's repeated, unauthorized access of medical records and human resource files at Employer A and Employer C were not minor offenses and neither event occurred under unique circumstances. When considered with his history of illegally downloading media and software as well as his prior viewing of pornographic material on a work computer, his actions reflect a history of non-compliance with basic rules and regulations and raise questions regarding his reliability, trustworthiness and judgment. Given the seriousness of his actions, Applicant has not met his burden to establish mitigation under either AG ¶¶ 17(c) or 17(d).

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 M, Guideline K, and Guideline E in my whole-person analysis.

On multiple occasions during two separate periods of time, Applicant breached the trust of his employers and the privacy of several individuals by viewing medical and human resource documents. He never informed the employers or the individuals of his actions. He also previously viewed pornography on a work computer and participated in the extensive illegal download of media and software. He now claims that he has matured and received training to be more cognizant of his obligations for the protection of information. However, given the seriousness of his conduct, particularly while he was employed as a system administrator, I find that Applicant has not met his burden of persuasion.

The record evidence leaves me with questions and doubts as to Applicant's suitability for a security clearance. I conclude that he failed to mitigate 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 E:	AGAINST APPLICANT
Subparagraph 1.a:	Against Applicant
Paragraph 2, Guideline M:	AGAINST APPLICANT
Subparagraphs 2.a-2.b:	Against Applicant
Paragraph 3, Guideline K:	AGAINST APPLICANT
Subparagraph 3.a:	Against Applicant

Conclusion

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

Bryan J. Olmos
Administrative Judge