DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 19-01585
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Alison O'Connell, Esq., Department Counsel
For Applicant: *Pro se*

08/19/2021

_____

Decision

_____

RICCIARDELLO, Carol G., Administrative Judge:

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

Statement of the Case

On June 28, 2019, the Department of Defense Consolidated Adjudication Facility issued to Applicant a Statement of Reasons (SOR) detailing security concerns under Guideline M, Use of Information Technology and Guideline E, Personal Conduct. The action was taken under Executive Order (EO) 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; DOD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the adjudicative guidelines (AG) effective within the DOD on June 8, 2017.

Applicant answered the SOR on August 2, 2019, and he requested a hearing before an administrative judge. This case was assigned to me on May 28, 2021. The notice of hearing was issued on June 28, 2021, scheduling the hearing, through the

Defense Collaboration System, for July 12, 2021. I convened the hearing as scheduled. The Government offered exhibits (GE) 1 through 5. Applicant objected to GE 4 and it was not admitted. Applicant and two witnesses testified on his behalf. He offered Applicant Exhibits (AE) A and B. There were no other objections and the remaining exhibits were admitted into evidence. DOHA received the hearing transcript on July 20, 2021.

Findings of Fact

Applicant denied the SOR allegations with explanations. After a thorough and careful review of the pleadings, testimony, and exhibits submitted, I make the following findings of fact.

Applicant is 40 years old. He earned a bachelor's and master's degrees in 2005 and 2007, respectively. He married in 2011 and adopted his wife's child, and they have three children from the marriage. He has worked for his current employer, a federal contractor, since July 2016. (Transcript (Tr.) 16-19, 43; GE 1)

Applicant worked at Company W from April 2015 to April 2016. He explained Company W grew while he was there from about 12 to 15 employees to about 20 to 30 employees. He explained the work environment changed. He applied for another job in March 2016 and received an offer on March 31, 2016. He completed his security clearance application on April 10, 2016. He testified that he had been vocal about business practices and was told that the company would not eliminate positions. He was terminated from his position on April 18, 2016. (Tr. 20-23)

Applicant testified that on the day he was terminated from his job he went to the office and observed that someone was at his workstation and on his computer. He was met by his supervisor and the director of human resources. He was told his position was being eliminated. He believed it was because he had been outspoken in the past. He said they had a civil and tense discussion. (Tr. 24-26)

Applicant testified that he went back to his office, collected his belongings, and left the building. He sat in his car and felt badly because he had unfinished work he intended to complete and work that he had not yet started that needed to be completed. This troubled him greatly because he is a professional and conscientious. He wanted to make sure his clients were treated correctly. (Tr. 25-27, 46)

Applicant then went home and accessed his home computer and through it he accessed a third-party software tracking program that had Company W's client's information. This is a project management program he used while working at Company W, which tracks the status of the work for each client. Applicant stated he did not access Company W's internal data system. He could only see the status of work that was to be done for the clients. He explained this was the only way he could attend to matters that he had meant to complete. He arranged client cards and assignments that needed to be updated or archived. He said there were things that had not been documented that

needed to be. He deleted six items that he said he had created. (Tr. 27-30, 44-49; GE 2, 3, 5)

Applicant testified that he did not have direct or indirect authorization to do any of these things. He was not granted approval by anyone at Company W to access the software or make any changes. No one explicitly gave him permission to do this. He said he left a voice mail for his supervisor, who had been present when he was terminated, and told her he was going to archive cards on the software that needed modification and taken off the action list. He said he also told a co-worker what he had done. He admitted that he was angry and upset after being terminated. He decided to access the software because it was the only way to make peace with what had happened and to make things right. He thought Company W was unfair and unjust and had done a disservice to the client. He was going to take the high road and make things right for the client. Before he logged in at home he did not contact anyone at Company W. (Tr. 27-35, 44-58; GE 2, 3, 5)

Applicant stated that when a card is archived it is no longer available at a specified location to determine its progress status. He archived 46 cards. By archiving a card, it is put in a different location. It is not deleted. Someone would not be able to find it where they normally expected it to be. He admitted it would be challenging for the next person working for a client to find their information if they did not know where the card was located. He admitted his actions made things more difficult for his successor. When asked why he archived a card when he could have notified someone that it was inaccurate. Applicant explained that he felt like it was up to him to do it. This was his work and responsibility, and he was going to clean it up. He did not have time to modify each card, so he chose to archive some and inform the supervisors later. When asked why not ask the supervisors first. He said because he did not think to do so. He said he thought professionally the client deserved to have the work performed properly, and he did not want to leave a bad impression. He stated that he felt like this was the best he could do to clean up work. He described it as putting things back in the file cabinet and not leaving things out on the table, figuratively speaking. (Tr. 35-40, 50-58, GE 2, 3, 5)

Applicant was interviewed by a government investigator in April 2017. Applicant was confronted with information that in about April 2016 he was terminated from employment at Company W and before the IT department deactivated access to one of the systems, Applicant had remotely accessed the system and began deleting data until another analysist discovered it, and Applicant's access was suspended. Applicant told the investigator it never happened. He said that he never remotely accessed any of Company W's systems. The only time his access was denied was the day he was terminated. He told the investigator that he was called and informed that he was going to be terminated. He could not provide any other information to the investigator with regards to his employment termination from Company W. (Tr. 35-40; GE 2)

Applicant explained at his hearing that he interpreted the investigator's questions as asking if he had accessed Company W's internal systems, which he said he had not. He admitted that the only Internet system he could access at home through Company W

was the third-party software. He said he did not think the third-party software, which he said was an external system, had anything to do with Company W's system. He thought the investigator had asked had he gone into Company W's system and deleted and manipulated data. He admitted he never provided clarification or explained the nuance he was relying upon to the investigator. He said he did not lie, but rather it was a misunderstanding. I did not find Applicant credible and find he deliberately misled the investigator by concealing his actions upon termination from employment with Company W. (Tr. 35-41, 58-61)

Applicant admitted he had pornography on his work computer. He admitted that it was "illicit material", and he believed it was against work policy to have it on his work computer. He downloaded photos from the Internet to his computer. He said the photos were boudoir photos of his wife and others. He liked them, so he kept them on his computer for access. When asked why he had illicit photos on his computer, he explained he thought they were nice, good photographic work, and he was able to view them as a break from work. He did not refer to the photos as pornography. (Tr. 61-65)

Applicant stated that he was not making good decisions while working at Company W. It was very stressful. He should not have had illicit material on his work computer. He should have gotten permission to access the software tied to Company W's clients. He is not proud of his conduct. He believed there was a misunderstanding between the government investigator and himself. (Tr. 66-68)

Two character witnesses testified on Applicant's behalf. His manager of two years stated that he has worked closely with him on projects as a mentor and technical advisor. He is dedicated to his work and his performance has been excellent. He is hard working, conscientious, and takes on many tasks and provides exemplary work. Applicant had discussed issues he had with his previous employer with the witness, but not the issues raised by the SOR. (Tr.71-75)

Another witness, who Applicant has worked for on military and sensitive projects, testified that Applicant has met all of the objectives of his work, on time and within budget. They deal with very complex tasks. Applicant is reliable and trustworthy. The witness was not aware of the contents of the SOR. (Tr. 77-78)

Policies

When evaluating an applicant's national security eligibility, the administrative judge must consider the AG. In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially disqualifying conditions and mitigating conditions, which are used in evaluating an applicant's eligibility for access to classified information.

These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, these guidelines are applied in conjunction with the factors listed in the adjudicative process. The administrative judge's overarching adjudicative goal is a fair, impartial, and commonsense decision. According to AG ¶ 2(c),

the entire process is a conscientious scrutiny of a number of variables known as the "whole-person concept." The administrative judge must consider all available, reliable information about the person, past and present, favorable and unfavorable, in making a decision.

The protection of the national security is the paramount consideration. AG ¶ 2(b) requires that "[a]ny doubt concerning personnel being considered for 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 avoided drawing 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. Directive ¶ E3.1.15 states 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 as to obtaining 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 an applicant may deliberately or inadvertently fail to safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation as to potential, rather than actual, risk of compromise of classified information.

Section 7 of EO 10865 provides that decisions shall be "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." *See also* EO 12968, Section 3.1(b) (listing multiple prerequisites for access to classified or sensitive information).

Analysis

Guideline M: Use of Information Technology

The security concerns relating to the guideline for use of information technology is set out in AG ¶ 39:

> Failure to comply with rules, procedures, guidelines, or regulations pertaining to information technology systems may raise security concerns about an individual's reliability and trustworthiness, calling into question the willingness or ability to properly protect sensitive systems, networks, and information. Information Technology includes any computer-based, mobile, or wireless device used to create, store, access, process, manipulate, protect, or move information. This includes any component, whether

integrated into a larger system or not, such as hardware, software, or firmware, used to enable or facilitate these operations.

AG ¶ 40 provides conditions that could raise security concerns. The following are potentially applicable:

(a) unauthorized entry into any information technology system;

(b) unauthorized modification, destruction, or manipulation of, or denial of access to, an information technology system or any data in such system; and

(e) unauthorized use of any information technology system

After being terminated from employment and without authorization, Applicant accessed Company W's client information from a third-party software program utilized by Company W from his home computer. He deleted and modified client information. Applicant also downloaded and stored illicit material on his work computer. There is sufficient evidence to support the application of the above disqualifying conditions.

The guideline also includes conditions that could mitigate security concerns arising from use of information technology. The following mitigating conditions under AG ¶ 41 are potentially applicable:

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

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

(c) The conduct was unintentional or inadvertent and was followed by a prompt, good-faith effort to correct the situation and by notification to appropriate personnel; and

(d) the misuse was due to improper or inadequate training or unclear instructions.

Applicant's conduct was deliberate and intentional. After being terminated he was angry. He repeatedly justified his conduct and indicated he was responsible for finishing work for clients that belonged to Company W after he was fired because he is a professional. He changed and manipulated data. He downloaded illicit photos of his wife and others onto his work computer because he liked to view them at work during his break. Applicant's conduct casts doubt on his reliability, trustworthiness, and good judgment. He was not authorized to make changes to client information after he was

terminated. His misuse was not minor. He did not make a good-faith effort to obtain authorization prior to accessing data from his home computer. None of the mitigating conditions apply.

Guideline E: Personal Conduct

AG ¶ 15 expresses the security concern for personal conduct:

> Conduct involving questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations can raise questions about an individual's reliability, trustworthiness and ability to protect classified information. Of special interest is any failure to provide truthful and candid answers during the security clearance process or any other failure to cooperate with the security clearance process. The following will normally result in an unfavorable national security eligibility determination, security clearance action, or cancellation of further processing for national security eligibility:

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

> (b) deliberately providing false or misleading information; or concealing or omitting information, concerning relevant facts to any 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
>
> (d) credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any other single guideline, but which, when considered as a whole, supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characterizes indicating that the individual may not properly safeguard classified of sensitive information.

Applicant accessed Company W's client information from his home computer after being terminated from employment. He downloaded and stored illicit photos on his work computer while working for Company W. These matters were alleged under Guideline M and cross-alleged under Guideline E. They have been adequately addressed under the Guideline M. AG ¶ 16(d) does not apply.

Applicant deliberately provided misleading information to a government investigator during his background interview by failing to explain and concealing the fact that he accessed Company W's client information from his home computer after being terminated, albeit from a third-party software program. He told the investigator that he

never remotely accessed any of Company W's systems. His explanation at his hearing that he did not access Company W's internal Internet without further explanation to the investigator was intentionally deceptive. He obviously was aware of what the government investigator's inquiries were about, yet concealed his involvement. He told the investigator that he could not provide any other information in regards to his termination. AG ¶ 16(b) applies.

The following mitigating conditions under AG ¶ 17 are potentially applicable to the disqualifying security concerns based on the facts:

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

Applicant did not make a good-faith effort to explain or correct what he described as a misunderstanding. His concealment was intentional, and his conduct was deceptive. Misleading a government investigator during a background interview for a security clearance is serious and casts doubt on Applicant's reliability, trustworthiness and good judgment. None of the above mitigating conditions apply.

Whole-Person Concept

Under the whole-person concept, the administrative judge must evaluate an applicant's eligibility for a security clearance by considering the totality of the applicant's conduct and all the 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 Guidelines M and E in my whole-person analysis.

Applicant has not met his burden of persuasion. The record evidence leaves me with serious questions and doubts as to Applicant's eligibility and suitability for a security clearance. For these reasons, I conclude Applicant failed to mitigate the security concerns arising under Guideline M, Use of Information Technology, and Guideline E, Personal Conduct.

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:	For Applicant
Subparagraph 2.b:	Against Applicant

Conclusion

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

_____
Carol G. Ricciardello
Administrative Judge