DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
.	)	ISCR Case No. 16-02940
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Nicole Smith, Esq., Department Counsel
For Applicant: Alan V. Edmunds

06/11/2018

_____

Decision

_____

LYNCH, Noreen A., Administrative Judge:

Applicant mitigated the security concerns under misuse of information technology and personal conduct. Eligibility for access to classified information is granted.

Statement of the Case

On April 3, 2017, in accordance with DoD Directive 5220.6, as amended (Directive), the Department of Defense issued Applicant a Statement of Reasons (SOR) alleging facts that raise security concerns under Guidelines M and E.[1] The SOR further informed Applicant that, based on information available to the government, DoD adjudicators could not make the preliminary affirmative finding it is clearly consistent with the national interest to grant or continue Applicant's security clearance.

[1] I considered the previous Adjudicative Guidelines, effective September 1, 2006, as well as the new Adjudicative Guidelines, (AG) effective June 8, 2017, which I applied in this case. My decision would be the same if the case was considered under the previous Adjudicative Guidelines.

Applicant answered the SOR on April 27, 2017, and requested a hearing before an administrative judge. (Answer.) The case was assigned to me on December 4, 2017. The Defense Office of Hearings and Appeals (DOHA) issued a notice of hearing on February 12, 2018, scheduling the hearing for April 10, 2018. The hearing was convened as scheduled. The Government offered Exhibits (GE) 1 through 4, which were admitted after Applicant offered clarifications on those documents. Applicant testified on his own behalf and presented 16 documents, which I marked Applicant's Exhibits (AE) A through P, and admitted. DOHA received the transcript of the hearing (Tr.) on April 18, 2018.

Findings of Fact

Applicant admitted the allegation in SOR ¶ 1.b. He denied SOR allegation ¶ 1.a and SOR ¶-2.b. After a thorough and careful review of the pleadings, exhibits, and testimony, I make the following findings of fact.

Applicant is a 36-year-old project manager of a defense contractor. He has been employed with the defense contractor since 2017. He received his undergraduate degree in 2004. (AE D) He held a security clearance for ten years. He is married, and has one son and one daughter. (AE J; K) Applicant completed his security clearance application (SCA) in October 2015. (GE 1)

The SOR alleges that in violation of company policy, Applicant loaded 551 megabytes of encrypted data onto his corporate computer system from a non-secure personal home network in approximately November 2014. (GE 3) When investigated, the uploaded data was found to contain pornographic material (GE 4). Applicant was terminated for the violations alleged in 1.a in or around February 2015. The SOR alleges that under personal conduct, 2.a, that Applicant falsified his 2015 SCA in response to Section 13A- Employment Activities for omitting the fact that he was terminated after uploading pornographic material to a government computer; and that under 2.b during a personal subject interview in November 2015 he provided false answers to an authorized investigator concerning his termination by omitting he uploaded pornographic material to a government computer. (GE 2)

Applicant disputed the term "corporate" computer, but acknowledged that he loaded encrypted data from a secure personal home network computer. In January 2015, his hard drive was removed from the government computer for investigation. downloaded. He further admitted that he loaded 551 megabytes of data, but not all was composed of pornographic material, if any, as suggested by the allegation. (Tr. 22) He claims he downloaded pictures of his wedding. He downloaded some on his lunchbreak. He stated it is highly possible that a few "unsavory" photos could have popped up based on a previous subscription to a men's digest website. He stated that sometimes when he followed that website, that pornographic windows and links, which were not blocked by DOD servers, would open up. (Answer)He said this is likely what happened, but he did not knowingly download 551 megabytes of pornographic material to his work computer.

Applicant no longer subscribes to the above-mentioned men's website and realizes that it was a foolish thing to access his personal home network from work. He views his home network as secure, but he no longer access anything from his home network from anything outside of his personal devices. He completed a cybersecurity awareness course in April 2017. (AE C)

As to SOR 1.b, Applicant admitted that he was terminated. He received two termination letters, both dated February 4, 2015. Each letter is written by the same person. One letter states that the termination is involuntary without cause due to lack of funding. The other letter, dated February 4, 2015, states that Applicant will be involuntarily terminated with cause for loading pornographic material on a government computer. It is not signed. (AE P)

When Applicant completed his October 2015 SCA, and answered Section 13A-Employment, he answered "Yes" he was fired due to misuse of government resources and also that he believed believed there were political issues. In his testimony, he stated that he did not intentionally falsify the SCA in this section because he believed that was a sufficient answer and one letter of his termination stated that he was terminated involuntarily without cause. In hindsight, he believes he should have added more information or been more specific and noted with cause.

When Applicant was interviewed in November 2015, he provided the investigator with the information that he knew. He noted that she was using an old SCA for the interview and noted that she needed to get the newest one. He stated that he was terminated for misuse of government computers.

Applicant submitted many awards and certificates from his years of employment with his former employer. (AE F) He also signed a statement of intent to not download unauthorized contents onto a government-owned computer. (AE B) He also submitted five letters of recommendation. He volunteers in the community. (AE G)

Policies

When evaluating an applicant's suitability for national security eligibility, the administrative judge must consider the pertinent AG. In addition to brief introductory explanations of the security concern, the guidelines list potentially disqualifying conditions and mitigating conditions, which are to be used in evaluating an applicant's national security eligibility.

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 AG ¶ 2 describing the adjudicative process. The administrative judge's overarching adjudicative goal is a fair, impartial, and commonsense decision. The entire process is a conscientious scrutiny of applicable guidelines in the context 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. I have not drawn inferences based on mere speculation or conjecture.

Directive ¶ E3.1.14 requires the Government to 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 the applicant or proven by Department Counsel, and has the ultimate burden of persuasion as to obtaining a favorable clearance decision."

A person applying for national security eligibility seeks to enter 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 national security eligibility. Decisions include, by necessity, consideration of the possible risk the applicant may deliberately or inadvertently fail to protect or safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation as to potential, rather than actual, risk of compromise of classified or sensitive information.

Finally, as emphasized in Section 7 of Executive Order 10865, "[a]ny determination under this order adverse to an applicant shall be a determination in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." *See also* Executive Order 12968, Section 3.1(b) (listing multiple prerequisites for access to classified or sensitive information.)

Analysis

Guideline M, Use of Information Technology

The security concern 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.

The 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.

While technically none of these exactly fir the nature of the case, these are Both potentially applkicablle.

AG ¶ 41 provides conditions that could mitigate security concerns. I considered all of the mitigating conditions under AG ¶ 41 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;

(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.

I find that AG ¶ 41(a) is applicable. The behavior happened under unusual circumstances several years ago and it was inadvertent. Applicant has worked with different government agencies for over ten years and has not had any violations. He believed he was uploading wedding pictures, but acknowledged that he followed a men's site that that sometimes pops up with unsavory pictures. He no longer follows that site. He took another cybersecurity course in April 2017. He signed a statement of intent to never misuse information technology or download unauthorized content onto government-owned computers. He has mitigated the concerns.

Guideline E, Personal Conduct

The security concern relating to the guideline for Personal Conduct 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:

> (a) refusal, or failure without reasonable cause, to undergo or cooperate with security processing, including but not limited to meeting with a security investigator for subject interview, completing security forms or releases, cooperation with medical or psychological evaluation, or polygraph examination, if authorized and required; and
>
> (b) refusal to provide full, frank, and truthful answers to lawful questions of investigators, security officials, or other official representatives in connection with a personnel security or trustworthiness determination.

The guideline notes several conditions that could raise security concerns under AG ¶ 16. These are potentially applicable in this case:

> (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;
>
> (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;
>
> (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;

(e) personal conduct, or concealment of information about one's conduct, that creates a vulnerability to exploitation, manipulation, or duress by a foreign intelligence entity or other individual or group. Such conduct includes:

> (1) engaging in activities which, if known, could affect the person's personal, professional, or community standing;
>
> (2) while in another country, engaging in any activity that is illegal in that country;
>
> (3) while in another country, engaging in any activity that, while legal there, is illegal in the United States;

(f) violation of a written or recorded commitment made by the individual to the employer as a condition of employment; and

(g) association with persons involved in criminal activity.

Applicant did not intentionally falsify his security clearance application in 2015. He listed that he was fired for misuse of government equipment. He received a letter of termination that stated that he was fired without cause for lack of funding .A second unsigned letter stated that he received another letter that spoke about the unearthing of pornographic material. He had no real knowledge of this. The record is murky and I do not find that he intentionally misled the Government.

Applicant noted in Section13A-Employment that he was fired. He believed it was for the misuse of his government equipment. He believed that was a sufficient answer. He stated that he was terminated for cause. In hindsight, he realizes that he could have

been more specific. I found his testimony credible. During his personal interview in 2015, the agent had an old SF-86. Applicant provided her with the recent one and pointed out that he had been fired for misuse of government computers. He answered every question that the agent asked. I find that Applicant did not intentionally falsify his SCA or the 2015 interview.

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 facts and circumstances surrounding this case. I have incorporated my comments under Guidelines M and E in my whole-person analysis. Some of the factors in AG ¶ 2(d) were addressed under those guidelines, but some warrant additional comment.

Applicant has a distinguished history of working in the defense industry and is respected by his employers. He performs well at his job. He is married and has two children. He has taken a cybersecurity course recently. He has held a security clearance for ten years. I found him credible in his testimony and demeanor.

Overall, the record evidence leaves me without questions or doubts as to Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude Applicant mitigated the Personal Conduct security concerns and Misuse of Technology concerns.

Formal Findings

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

Paragraph 1, Guideline M: FOR APPLICANT

Subparagraphs 1.a-b:	For Applicant
Paragraph 2, Guideline E:	FOR APPLICANT
Subparagraphs 2.a-2b:	For Applicant

Conclusion

In light of all of the circumstances presented by the record in this case, it is clearly consistent with the national interest to grant Applicant eligibility for a security clearance. Eligibility for access to classified information is granted.

_____
Noreen A. Lynch
Administrative Judge