DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 18-02588
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Kelly Folks, Esq., Department Counsel
For Applicant: *Pro se*

12/19/2019

_____

Decision

_____

RIVERA, Juan J., Administrative Judge:

Applicant's evidence is insufficient to mitigate the personal conduct and use of information technology security concerns. Clearance is denied.

Statement of the Case

Applicant was the subject of a Security Access Eligibility Report (SAER) for inappropriate use of web services, dated May 15, 2017. He submitted his most recent security clearance application (SCA) on July 14, 2017. He was interviewed by government investigators on April 16, 2018, and answered a set of interrogatories from the Defense Office of Hearings and Appeals (DOHA) on February 23, 2019. After reviewing the information gathered during the background investigation, the Department of Defense (DOD) issued a Statement of Reasons (SOR) on April 4, 2019, alleging security concerns under Guidelines E (personal conduct) and M (use of information technology). Applicant answered the SOR on May 8, 2019, and requested a hearing before a DOHA administrative judge.

DOHA assigned the case to me on August 2, 2019, and issued a notice of hearing on August 13, 2019, setting the hearing for September 12, 2019. At the hearing,

the Government offered four exhibits (GE 1 through 4). GE 1, 2, and 4 were admitted into the record without any objections. Applicant's objection to GE 3 (that the document was incomplete because it did not specify the number of times the adult sites were accessed) was overruled, and I admitted the document as evidence. Applicant testified on his own behalf and presented the testimony of two witnesses and four character statements, all of which I admitted into the record without any objections. I marked the Government's discovery letter as Hearing Exhibit 1. DOHA received the hearing transcript (Tr.) on September 20, 2019.

Findings of Fact

Applicant denied the two SOR allegations (¶¶ 1.a and 2.a) with mitigating comments. After a thorough review of the record evidence, I make the following findings of fact:

Applicant is a 40-year-old employee of a federal contractor. He received his high school diploma in 1997, and completed some college courses between 2003 and 2005, but did not earn a degree. He enlisted in the Army in 1997; served honorably on active duty between 1998 and 2001; and in the Inactive Reserve between 2001 and 2005. Applicant married his wife in 2000. They have a son, who is almost two years old.

Applicant has been working for federal contractors since he was discharged from active duty in 2001. He held a top-secret clearance between October 2011 and June 2017. He was laid off from his job in June 2017 as a result of the SOR allegations. He seeks the reinstatement of his clearance eligibility, which is required for his employment with a federal contractor.

Applicant's security concerns arose because of his inappropriate use of web services. In February and, in particular, on April 28, 2017, a computer program alerted Applicant's agency's computer network defense (CND) team of his repeated access to multiple pornographic images and inappropriate content. An investigation into Applicant's web traffic patterns for April 2017 identified the inappropriate web sites he visited and images he accessed. Additionally, the investigation found saved in Applicant's computer inappropriate images and a sexually explicit conversation with a co-worker. (GE 3)

Applicant denied that he inappropriately used his employer's government information technology system to view inappropriate content. He admitted that his common access card (CAC) was used to access the inappropriate sites, but claimed that he left his CAC in his computer when going to meetings or the bathroom, and that co-workers must have accessed the improper sites without his knowledge to get him in trouble.

Applicant presented the testimony of a co-worker (F) to show that other employees had accessed her computer and used it to send unwanted email messages

to others as a joke when she went to the bathroom. She explained that the computers were old and failed to log you out immediately. Applicant believes that the same happened to him, and someone accessed the improper sites when he was not at his computer. However, his beliefs are unsubstantiated.

At his hearing, Applicant admitted that he entered into an inappropriate email conversation with a co-worker, and that he saved a copy of the email correspondence in his computer. He acknowledged his lack of judgment and expressed sincere remorse for his behavior.

Applicant's references (supervisors and co-workers) are impressive. They attest to Applicant's professionalism and unwavering moral character. They consider Applicant to have unique analytical skills, knowledge, and a strong sense of team work. He consistently outperform his co-workers with quality products through sound research skills and attention to detail. He is considered to be the top one-percent producer, and a critical member of the organization analytical production team. He demonstrated strong leadership and was appointed as the site lead. He excelled mentoring junior analysts and providing training. Because of his outstanding contributions he was appointed senior analyst.

Applicant's references are aware of the SOR allegations. They found the behavior completely out of character for someone with Applicant's 20-year of proven performance record. They recommended Applicant's continued eligibility for a clearance.

Policies

The SOR was issued under Executive Order 10865, *Safeguarding Classified Information Within Industry* (February 20, 1960), as amended; DOD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (Directive) (January 2, 1992), as amended; and the *National Security Adjudicative Guidelines for Determining Eligibility for Access to Classified Information or Eligibility to Hold a Sensitive Position* (AGs), applicable to all adjudicative decisions issued on or after June 8, 2017.

Eligibility for access to classified information may be granted "only upon a finding that it is clearly consistent with the national interest to do so." Exec. Or. 10865, *Safeguarding Classified Information within Industry* § 2 (Feb. 20, 1960), as amended. The U.S. Supreme Court has recognized the substantial discretion of the Executive Branch in regulating access to information pertaining to national security, emphasizing that "no one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988).

The AG list disqualifying and mitigating conditions for evaluating a person's suitability for access to classified information. Any one disqualifying or mitigating

condition is not, by itself, conclusive. However, the AG should be followed where a case can be measured against them, as they represent policy guidance governing access to classified information. Each decision must reflect a fair, impartial, and commonsense consideration of the whole person and the factors listed in SEAD 4, App. A ¶¶ 2(d) and 2(f). All available, reliable information about the person, past and present, favorable and unfavorable, must be considered.

Security clearance decisions resolve whether it is clearly consistent with the national interest to grant or continue an applicant's security clearance. The Government must prove, by substantial evidence, controverted facts alleged in the SOR. If it does, the burden shifts to the applicant to rebut, explain, extenuate, or mitigate the facts. The applicant bears the heavy burden of demonstrating that it is clearly consistent with the national interest to grant or continue his or her security clearance.

Persons with access to classified information enter into a fiduciary relationship with the Government based on trust and confidence. Thus, the Government has a compelling interest in ensuring each applicant possesses the requisite judgment, reliability, and trustworthiness of those who must protect national interest as their own. The "clearly consistent with the national interest" standard compels resolution of any reasonable doubt about an applicant's suitability for access in favor of the Government. "[S]ecurity clearance determinations should err, if they must, on the side of denials." *Egan*, 484 U.S. at 531; SEAD 4, ¶ E(4); SEAD 4, App. A, ¶¶ 1(d) and 2(b). Clearance decisions are not a determination of the loyalty of the applicant concerned. They are merely an indication that the applicant has or has not met the strict guidelines the Government has established for issuing a clearance.

Analysis

Guideline E: Personal Conduct

AG ¶ 15 sets forth the security concern as follows:

> 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 . . . .

The record evidence establishes that between February and April 2017, Applicant inappropriately used his employer's government information technology system to view inappropriate content, and that he engaged in inappropriate explicit correspondence with a co-worker on a government system. Applicant's behavior raises the following disqualifying condition under AG ¶ 16:

> (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 . . . .

The record established the above disqualifying condition, requiring additional inquiry about the possible applicability of the mitigating conditions. I considered the following mitigating conditions set forth by AG ¶ 17 as partially raised by the evidence:

> (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;
>
> (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; and
>
> (e) the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress.

After analyzing the above mitigating conditions in light of the record evidence as a whole, I find that they are not applicable and do not mitigate the personal conduct concerns. Considering Applicant's service and professional experience, I cannot find his behavior a minor offense. Because of his work experience and leadership position, he knew it was inappropriate to use government equipment to access inappropriate information or content on the Internet. Similarly, I consider his questionable behavior recent and frequent (although limited to a two-month period). I also find that Applicant's questionable behavior still casts doubt on his reliability, trustworthiness, and good judgment.

I carefully considered Applicant's assertion that, unbeknown to him, co-workers who wanted to harm him, used his CAC card to access and view inappropriate sites and content. In light of the information technology investigation report, I find Applicant's contentions not persuasive or credible. The investigation report is extensive, detailed, and specific as to the multiple number of sites and inappropriate content that Applicant accessed. Applicant failed to rebut the Government's evidence.

Applicant denied the allegations against him and he has not participated in counseling. AG ¶ 17(d) is not applicable. Considering the evidence as a whole, I find that the Guideline E allegations continue to raise concerns under AG ¶ 16(e), which are not mitigated.

Guideline M, Use of Information Technology

AG ¶ 39 describes the security concern for 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.

Under Guideline M, the SOR cross-alleged the same facts and circumstances alleged under Guideline E. For the sake of brevity, the facts, analysis, and conclusions outlined under Guideline E are incorporated herein without repeating them.

AG ¶ 40 lists a condition that could raise a security concern and may be disqualifying:

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

Between February and April 2017, Applicant used his employer's government information technology system to view inappropriate content, and he engaged in inappropriate explicit correspondence with a co-worker. Because of his training, service, and professional experience, Applicant knew that accessing inappropriate sites and content through government equipment was prohibited under security rules and procedures. He acknowledged he displayed lack of judgment when he engaged in inappropriate explicit correspondence with a co-worker. AG ¶ 40(e) is established.

AG ¶ 41 provides conditions that could mitigate security concerns:

> (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; and

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

For the same reasons stated under Guideline E, incorporated herein, Applicant failed to submit sufficient evidence to mitigate the use of information technology systems security concerns.

Whole-Person Concept

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

Applicant, 40, honorably served in the U.S. military. He has been employed with federal contractors since he was discharged from the service in 2001. He held a clearance, at least between 2001 and 2017, without any security incidents of concern, except for the SOR allegations.

Applicant's references' statements in support of him are impressive. They attest to his professionalism and unwavering moral character. He is considered to have unique analytical skills, knowledge, and a strong sense of team work. He consistently outperform his co-workers with quality products through sound research skills and attention to detail. He is considered to be the top one-percent producer, and a critical member of his organization's analytical production team. He demonstrated strong leadership and was appointed as the site lead and senior analyst. Applicant's references are aware of the SOR allegations. They found the behavior completely out of character. They recommended Applicant's continued eligibility for a clearance.

Nevertheless, it is well settled that once a concern arises regarding an applicant's security clearance eligibility, there is a strong presumption against granting a security clearance. Unmitigated security concerns lead me to conclude that granting a security clearance to Applicant is not warranted at this time.

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
Subparagraph 2.a:	Against Applicant

Conclusion

In light of all the circumstances presented by the record in this case, it is not clearly consistent with the national security interests of the United States to continue Applicant's eligibility for a security clearance. Clearance is denied.

_____
JUAN J. RIVERA
Administrative Judge