



**DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS**



In the matter of:)	
)	
[REDACTED])	ISCR Case No. 20-01815
)	
Applicant for Security Clearance)	

Appearances

For Government: Brian Olmos, Esq., Department Counsel
 For Applicant: *Pro se*
06/24/2021

Decision

MARINE, Gina L., Administrative Judge:

This case involves security concerns raised under Guideline M (Use of Information Technology) and Guideline E (Personal Conduct). Eligibility for access to classified information is denied.

Statement of the Case

Applicant submitted a security clearance application on May 13, 2019 (2019 SCA). On October 28, 2020, the Defense Counterintelligence and Security Agency Consolidated Adjudications Facility (CAF) sent him a Statement of Reasons (SOR) alleging security concerns under Guidelines M and E. The CAF acted under Executive Order (EO) 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; Department of Defense (DOD) Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the adjudicative guidelines (AG) implemented by the DOD on June 8, 2017.

Applicant answered the SOR on October 28, 2020, and requested a decision based on the written record in lieu of a hearing. On December 22, 2020, the Government sent Applicant a complete copy of its written case, a file of relevant material (FORM), including pleadings and evidentiary documents identified as Items 1 through 8. He was given an opportunity to submit a documentary response setting forth objections, rebuttal, extenuation, mitigation, or explanation to the Government’s evidence. He received the

FORM on January 7, 2021, and timely submitted a response, to which the Government did not object. Applicant did not object to any of the Items included in the FORM. The case was assigned to me on February 10, 2021.

Evidentiary Matters

Items 1 and 2 contain the pleadings in the case. Items 3 through 8 are admitted into evidence. Applicant's SOR Answer included evidentiary documents that I admitted into evidence as Applicant Exhibits (AE) A through C. Item 6 was not authenticated as required by Directive ¶ E3.1.20. However, I conclude that Applicant waived any objection to Item 6. The Government included in the FORM a prominent notice advising Applicant of his right to object to the admissibility of Item 6 on the ground that it was not authenticated. Applicant was also notified that if he did not raise an objection to Item 6 in his response to the FORM, or if he did not respond to the FORM, he could be considered to have waived any such objection, and that Item 6 could be considered as evidence in his case. Applicant did not object to Item 6 in his FORM response or otherwise.

Findings of Fact

Applicant, age 34, is married with four minor children. He earned a bachelor's degree in 2012. He has been employed as an engineer by a defense contractor since March 2019. He was previously granted security clearances in 2012 and 2016. (Item 5)

The SOR alleged facts regarding misconduct that resulted in Applicant being terminated by Employer 1 in 2015 (SOR ¶¶ 1.a and 2.a.) and by Employer 2 in 2018 (SOR ¶ 2.b). In his SOR answer, Applicant admitted each allegation and proffered mitigating evidence. Despite his admission and references to being terminated by Employer 1 throughout the security clearance process, I have construed his 2015 termination as a "resignation in lieu of termination" to conform to the record evidence, an official business record stating same. (Item 2; Item 7 at 29)

Applicant worked for Employer 1, as a government contractor, for three years until he resigned in lieu of being terminated for cause in October 2015 after violating company policies relating to computer misuse and labor mischarging. He misused his company-issued computer by accessing sexually explicit materials. He mischarged labor hours to the U.S. government for time that he was actively engaged in excessive personal use on his company-issued computer. These incidents occurred while Applicant was at his workplace during the workday. (AE A; Item 7 at 29; Items 5, 8)

A coworker, who observed Applicant viewing nude images on two occasions, reported both incidents to Applicant's supervisor. Following the initial incident in June 2015, the supervisor counseled Applicant about the appropriate use of company assets and labor charging. The supervisor assumed Applicant had corrected the behavior until he was notified of the second incident in August 2015, at which time Employer 1 initiated an investigation, including active desktop monitoring (ADM) for a period of nine days. (Items 5, 8)

The investigation confirmed the August 2015 incident. The ADM revealed that Applicant: 1) accessed nude and/or sexually explicit images on seven of the nine days; 2) was actively engaged in an excessive amount of other non-work web activity over nine days; and 3) took deliberate actions to conceal his internet searches and other web activity. Employer 1 concluded that Applicant mischarged roughly 42% of his time, which equated to 158 hours between the date the allegations were first reported and his last day of employment. His mischarging, which resulted in a loss of approximately \$13,874, included the time he spent on viewing sexually explicit materials and other non-work web activity on his company-issued computer. (AE B; Item 7 at 13-30; Item 8)

Applicant knew at the time he was accessing sexually explicit materials that it was against company policy. He initially denied that he mischarged his labor hours believing that the time he spent on non-work activity was acceptable because it occurred during what he considered downtime. However, he eventually acknowledged that he was mistaken in that belief, accepted responsibility for his actions, and recognized the seriousness of his misconduct. (FORM Response; Item 8 at 7)

Applicant attributed his 2015 misconduct to an addiction he had to pornography and sexually explicit materials since he was a teenager. He resorted to it as a “mental escape” when faced with challenges at home or work. He had been in denial that he had a problem until he was faced with termination. He has since sought and received counseling on a regular basis, and developed strategies to help him to overcome his addiction and prevent relapse. He increased his involvement in serving his community. In August 2017, Applicant’s counselor expressed his belief that Applicant would make a full recovery. (AE B; Item 2; Item 7 at 7, 29-30; Item 8 at 11-13; FORM Response)

In July 2017, the Department of the Navy notified Applicant of his proposed debarment on the basis of his significant mischarging in 2015. In September 2017, Applicant successfully appealed the debarment. The SDO (Suspending and Debarring Official) concluded that Applicant appreciated the gravity of the misconduct that formed the basis of the proposed debarment, and took steps to correct his behavior to ensure appropriate future conduct. The SDO believed that Applicant no longer presented a threat to the integrity of the government procurement process. (AE B; Item 7 at 13-30)

Applicant worked for Employer 2 for 23 months until he was terminated for cause in February 2018, during his probationary period, after his performance and conduct were deemed unacceptable. The following summarized the incidents upon which his termination was based: 1) continuously demonstrated a lack of teamwork and cooperation with his coworkers; 2) continuously engaged in an argumentative and discourteous manner toward others; 3) routinely made decisions on issues that he was unwilling to discuss when there were differences in opinion; and 4) unwilling to be collaborative, which negatively impacted productivity and the mission. (Item 7 at 31-49)

In February 2018, Applicant received a notice outlining the basis of his termination, including the specific incidents noted above. He was informed of his right to grieve the action, of which he timely availed himself. However, his grievance was later cancelled

due to an administrative oversight. He was also advised of a separate right to appeal the action. There is no indication in the record that he did so. (Item 7 at 44-49)

Applicant attributed his 2018 termination to his inability to effectively communicate. He denied any malicious intent and expressed regret for having never been given the opportunity to explain himself before being terminated. He has since received counsel from his spouse and friends to better understand more effective ways of interacting with coworkers. He has learned to be a better coworker, sought to listen and follow more, and show more trust and patience with his chain of command. He has implemented techniques to help him to be a better employee. He asserted that his current employer has recognized his growth as an employee. (AE C; Item 2 at 3; Item 7 at 9, 30; FORM response)

Throughout the security clearance process, Applicant equivocated the derogatory details surrounding his 2015 misconduct. He omitted the fact that he viewed sexually explicit materials and mischarged labor when reporting the 2015 termination on his February 2016 Declaration for Federal Employment, March 2016 SCA, and during his May 2016 security clearance interview. On his May 2019 SCA, he disclosed that he viewed “explicit material,” but not that he mischarged time; only that it was reported as such. During his July 2019 security clearance interview, he stated that he was terminated for mischarging time and that “pornography was found on his work computer.” After being confronted during his December 2019 security clearance interview, Applicant acknowledged that he had not gone into “extensive detail” about the actual reasons for his 2015 termination “due to the embarrassing nature of situation.” He also claimed that he did not recall the specific details involved. (Items 3-6; Item 7 at 5, 9)

Applicant understated the reasons for his 2018 termination on his May 2019 SCA and during his July 2019 interview. When explaining the reason for his termination on the SCA, he stated: “Supervisor suggested that I [was] not a good fit for position . . . it was reported that I did not fit the temporary assignment and tasks at hand.” During the interview, he asserted that he was unsure why he was terminated beyond being told by his supervisor that that he was simply not a good fit. While he claimed that he did not recall the official reason given to him for his termination, he asserted that it was not due to any fault of his own. After being confronted during his December 2019 security clearance interview, Applicant claimed that he listed what he believed to be the official reason for the termination. He asserted that he did not list “all the specific details due to not knowing an official reason.” (Item 5 at 18; Item 7 at 4-5, 7)

In his FORM response, Applicant expressed remorse for what he described as miscommunicating the severity of the circumstances surrounding his 2015 misconduct. He stated that he was “not proud of this choice/issue,” and admitted:

I was afraid. Each time I discussed this incident I felt I could never grow beyond it. I felt like I was branded and could never be trusted again . . . My fear of reprisal of fully saying every detail kept me from full reporting. I was unaware fully of the government desire to see the total person. [T]his was a grave error. [L]ooking back, I remember being told about the total

person review, yet I still was afraid of my past. I am deeply upset I couldn't just state the facts. . . .

He also apologized for not providing the specific issues underlying his 2018 termination, which he attributed to miscommunication and a misunderstanding of the reporting requirements. In support of mitigation, Applicant stated:

My spouse, current management, and religious leaders are aware of these situations and have helped me be a better person. They stand as a help to me against exploitation, manipulation, and duress anyone would attempt to do to get me to act contrary to complete loyalty to the United States Government and her mission. As each day goes by, I remember my lack of candor and lack of obedience[.] I work each day to be better. I do not dismiss the actions I did. Each day I try to be better.

Between 2016 and 2020 Applicant satisfactorily completed approximately 15 trainings, which included the topics of ethics, security, and integrity. (AE C).

Policies

“[N]o one has a ‘right’ to a security clearance.” (*Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988)). As Commander in Chief, the President has the authority to “control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to have access to such information.” (*Egan* at 527). The President has authorized the Secretary of Defense or his designee to grant applicants eligibility for access to classified information “only upon a finding that it is clearly consistent with the national interest to do so.” (EO 10865 § 2).

Eligibility for a security clearance is predicated upon the applicant meeting the criteria contained in the AG. These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, an administrative judge applies these guidelines in conjunction with an evaluation of the whole person. An administrative judge’s overarching adjudicative goal is a fair, impartial, and commonsense decision. An administrative judge must consider all available and reliable information about the person, past and present, favorable and unfavorable.

The Government reposes a high degree of trust and confidence in persons with access to classified information. This relationship transcends normal duty hours and endures throughout off-duty hours. Decisions include, by necessity, consideration of the possible risk that the applicant may deliberately or inadvertently fail to safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation about potential, rather than actual, risk of compromise of classified information.

Clearance decisions must be made “in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned.” (EO 10865 § 7). Thus, a decision to deny a security clearance is merely an indication the applicant has

not met the strict guidelines the President and the Secretary of Defense have established for issuing a clearance.

Initially, the Government must establish, by substantial evidence, conditions in the personal or professional history of the applicant that may disqualify the applicant from being eligible for access to classified information. The Government has the burden of establishing controverted facts alleged in the SOR. (*Egan*, 484 U.S. at 531). “Substantial evidence” is “more than a scintilla but less than a preponderance.” (*See v. Washington Metro. Area Transit Auth.*, 36 F.3d 375, 380 (4th Cir. 1994)). The guidelines presume a nexus or rational connection between proven conduct under any of the criteria listed therein and an applicant’s security suitability. (ISCR Case No. 92-1106 at 3, 1993 WL 545051 at *3 (App. Bd. Oct. 7, 1993)). Once the Government establishes a disqualifying condition by substantial evidence, the burden shifts to the applicant to rebut, explain, extenuate, or mitigate the facts. (Directive ¶ E3.1.15). An applicant has the burden of proving a mitigating condition, and the burden of disproving it never shifts to the Government. (ISCR Case No. 02-31154 at 5 (App. Bd. Sep. 22, 2005)).

An applicant “has the ultimate burden of demonstrating that it is clearly consistent with the national interest to grant or continue his security clearance.” (ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002)). “[S]ecurity clearance determinations should err, if they must, on the side of denials.” (*Egan*, 484 U.S. at 531; AG ¶ 2(b)).

Analysis

Guideline M: Use of Information Technology

The security concern under 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.

Applicant’s admissions and the documentary evidence establish the following disqualifying conditions under this guideline:

AG ¶ 40(e): unauthorized use of any information technology system; and

AG ¶ 40(g): negligence or lax security practices in handling information technology that persists despite counseling by management.

Of the conditions that could mitigate the concern under this guideline, the following is potentially applicable:

AG ¶ 41(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 knew he was violating company policy when he accessed sexually explicit materials on his company-issued computer while at his workplace during the workday. He accessed those materials on a regular basis, including after being counseled by his supervisor. He was actively engaged in excessive personal use on his company-issued computer, which he deliberately acted to conceal. While these were serious offenses, they occurred over five years ago and are not likely to recur. However, AG ¶ 41 (a) is not established because his repeated and recent efforts to obscure the derogatory details of his 2015 misconduct out of fear and embarrassment continues to cast doubt on his current reliability, trustworthiness, and good judgment. To the extent that his counseling has helped him overcome his admitted addiction to pornography, his lack of candor about his misconduct undermines mitigation of his misuse of information technology.

Guideline E: Personal Conduct

The concern under this guideline, as set out in AG ¶ 15, includes: "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."

Applicant's admissions and the documentary evidence establish the general concerns involving questionable judgment and unwillingness to comply with rules and regulations and the following specific disqualifying conditions under this guideline:

AG ¶ 16(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.

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;

Of the conditions that could mitigate the concern under this guideline, the following are potentially applicable:

AG ¶ 17(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;

AG ¶ 17(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

AG ¶ 17(e): the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress.

Applicant's 2015 misconduct was serious and is also disqualifying under this guideline. While the specific behaviors underlying Applicant's 2018 termination were less serious by comparison, they denote an ongoing pattern of questionable judgment and inappropriate behavior that further exacerbates the concern. Applicant damaged his credibility, during his December 2019 interview, when he claimed not to know the "specific details" of his 2015 misconduct or the "official reason" for his 2018 termination. He would have been well aware of the details during his 2017 debarment appeal. Similarly, in 2018, he not only was provided with an official notice detailing the reasons but also participated in the grievance process. His professed remorse for his actions and rehabilitation appear sincere. However, his repeated and recent efforts to minimize and obscure the derogatory details of the facts and circumstances underlying his 2015 resignation and 2018 termination during the security clearance process diminished the weight of the evidence of reform. Applicant failed to demonstrate a sufficient pattern of responsible behavior. In light of these circumstances, I am unable to conclude that Applicant's questionable judgment and rules violations are unlikely to recur. I have doubts about Applicant's current reliability, trustworthiness, and good judgment. None of the mitigating conditions under AG ¶ 17 fully apply.

Whole-Person Concept

Under AG ¶ 2(c), the ultimate determination of whether the granting or continuing of national security eligibility is clearly consistent with the interests of national security must be an overall common sense judgment based upon careful consideration of the adjudicative guidelines, each of which is to be evaluated in the context of the whole person. In evaluating the relevance of an individual's conduct, an 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.

I have incorporated my comments under Guidelines M and E in my whole-person analysis, and considered the factors in AG ¶ 2(d). After weighing the disqualifying and mitigating conditions under Guidelines M and E, and evaluating all the evidence in the context of the whole person, I conclude that Applicant has not mitigated security concerns involving his use of information technology and his personal conduct. Accordingly, Applicant has not carried his burden of showing that it is clearly consistent with the interests of national security to grant him eligibility for access to classified information.

Formal Findings

Formal findings 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:	Against Applicant
Subparagraph 2.b:	Against Applicant

Conclusion

I conclude that it is not clearly consistent with the interests of national security to grant Applicant eligibility for access to classified information. Clearance is denied.

Gina L. Marine
Administrative Judge