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

| | | |
|---|---|---|
| In the matter of: | ) | |
| | ) | |
| | ) | ISCR Case No. 19-01491 |
| | ) | |
| Applicant for Security Clearance | ) | |

## Appearances

For Government: Andrea Corrales, Esq., Department Counsel
For Applicant: *Pro se*

01/19/2022

_____

## Decision

_____

CERVI, Gregg A., Administrative Judge

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

## Statement of the Case

Applicant submitted a security clearance application (SCA) on January 12, 2018. On September 2, 2020, Department of Defense Counterintelligence and Security Agency, Consolidated Adjudications Facility (DCSA CAF) sent him a Statement of Reasons (SOR) alleging security concerns under Guidelines E and M. The DCSA CAF acted 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 adjudicative guidelines (AG) effective on June 8, 2017.

Applicant replied to the SOR in an undated response, and requested a hearing before an administrative judge. The case was assigned to me on August 26, 2021. The Defense Office of Hearings and Appeals (DOHA) issued a notice of hearing on

September 9, 2021, and the hearing was convened on September 17, 2021. A witness for the government testified, and Government Exhibits (GE) 1 through 8 were admitted in evidence. Applicant testified and submitted Applicant's Exhibit (AE) A, which was admitted. DOHA received the hearing transcript (Tr.) on September 27, 2021.

## Findings of Fact

Applicant is a 38-year-old training and development specialist, employed by a defense contractor. He previously worked for another defense contractor from April 2016 to March 2017, until he was terminated for violating timekeeping and information systems security policies. He was also employed as a United States Secret Service uniformed division officer from 2008 to 2010. He received a bachelor's degree in 2006. He married in 2008 and divorced in 2014. He remarried in November 2018. He has three children, ages 18 months, 10, and 14 years old. He holds a top secret security clearance.

The SOR alleges under Guideline E that Applicant was terminated from his employment with a government contractor in March 2017 for violating timekeeping and information systems security policies. Under Guideline M, the SOR cross-alleges Applicant's termination for violating information systems security policy. Applicant initially admitted the Guideline E allegation, but denied the Guideline M allegation. At the hearing, he changed his answer on the Guideline M allegation to "admit."

Applicant was employed by a company that directly supported another government agency, by researching classified computer databases in a sensitive compartmented information facility (SCIF) in which he was required to "badge in" to gain access. All work had to be conducted in the SCIF. Applicant was to account for his time and attendance by logging his work time daily on an unclassified computer database, in 15-minute increments. The timekeeping program could be accessed anywhere on a personal computer, including at Applicant's home. The system employed a unique username and password, and only the employee was permitted to sign in and use the system. If an employee could not enter the data, he was required to call or email his supervisor, or send a note through the timekeeping system. The employee's input would be used to charge the government customer under the contract. Applicant was also required to report his time on a classified system in the SCIF, to include noting on the government customer's calendar when he expected to be out of the office or unable to work normal work hours. Employees were required to keep the calendar updated. Applicant was trained on the timekeeping system and information security requirements.

In late 2016, the government supervisor in the SCIF notified Applicant's senior program manager of concerns over Applicant's extended breaks and arriving to work late or leaving early. The manager asked the SCIF supervisors to make notes and observe Applicant's conduct. It was discovered that between January and February 2017, Applicant falsified his timecard by logging work that was not performed for seven days. The missed work was improperly billed to the government. In addition, the company determined that Applicant did not "badge in" to the SCIF on six days for which he entered work hours. The manager confronted Applicant about the falsified timecards, and he

denied it, but admitted to improperly certified working on two days that he did not work. Applicant did not elaborate on missed work or claim that he worked on alternate times or days to make up for missed regular workdays. The manager believed Applicant was lying about only falsifying two days of missed work.

The company conducted an internal audit and Applicant was interviewed. Applicant admitted fraudulently certifying working two days that he did not work. He also admitted to giving his username and password to his girlfriend (now his spouse), to log into the timekeeping system and sending a certification of his work performed for the week. As a result, Applicant was placed on administrative leave, was "read off" the program, and barred from the SCIF. The manager notified Applicant that he was being terminated. Applicant never contested his termination with the company because he agreed that he mischarged two days and improperly allowed his girlfriend to certify his work hours.

In testimony, Applicant continued to assert that he mischarged only two days, but corrected his timecard the following week to take leave. He stated that he had no desire to contest his termination from the company because he agreed that he initially mischarged the two days and allowed his girlfriend to submit his timecard. He also admitted to following another employee into the SCIF without "badging in," as a way to account for the inability of the system to show he was present in the SCIF, however he later denied it in testimony, claiming that he always "badged in" even when he walked in behind another employee.

Applicant claimed that he went to the emergency room in late February 2017, and was required to undergo an emergency procedure. He first testified that it was February 4th or 5th, then said it was the week of February 9th or 10th. His girlfriend took him to the hospital on a Wednesday evening after work for a test when he learned that he needed a procedure. At his direction, she returned home to open his laptop timekeeping program in which he had already logged in and pre-populated the fields with his work time for the week, and hit "send" on the program. She then returned to the hospital. Applicant admitted to regularly pre-populating his timecard before working the hours. When his girlfriend certified his timecard for him, he had populated work for the full week although he certified the timecard on a Wednesday evening. In testimony, Applicant claimed he regularly populated the entire work week on his timecard submissions, typically sent on Thursdays, but he did not know he had populated the entire week when he asked his girlfriend to certify his work. Applicant claimed that he asked her to certify it on Wednesday evening, even though he normally submitted it on Thursdays, because he did not know how long he would be in the hospital. He also stated that he could have accessed the program on his cell phone while in the hospital, but he was "out of it" and in too much pain to do so.

Applicant produced character letters from friends and community leaders attesting to his honesty, reliability, family focus, and community involvement. He did not produce documentary evidence to support his claims regarding timekeeping or his hospital visit, nor did he produce his spouse or other witnesses to testify as to the events the evening

he went to the hospital, company's timekeeping policies, SCIF entry practices, and work schedules.

## 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." *Id.* 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." Exec. Or. 10865 § 2.

National security eligibility is predicated upon the applicant meeting the criteria contained in the adjudicative guidelines. 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 a person's stability, trustworthiness, reliability, discretion, character, honesty, and judgment. AG ¶ 1(b).

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." Exec. Or. 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. *See, e.g.,* ISCR Case No. 12-01295 at 3 (App. Bd. Jan. 20, 2015).

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. *See, e.g.,* 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; *see,* AG ¶ 1(d).

## Analysis

### Guideline E: Personal Conduct

The concern under 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.

The relevant disqualifying conditions under AG ¶16 are:

> (c) credible adverse information in several adjudicative issues 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; and
>
> (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:
>
> . . .
>
> (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 admissions and the evidence support a finding of questionable judgment, dishonesty, company policy violations, and misuse of the government's and his employer's time and resources. AG ¶¶ 16(c) and (d) apply.

Conditions that could mitigate personal conduct security concerns are provided under AG ¶ 17. 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;
>
> (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 caused 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.

Applicant's conduct, taken as a whole, shows the wrongful use of the company's timekeeping policies to permit his girlfriend to certify his time that he knew or should have known was incorrect, and repeated mischarging of time that was not worked. He admitted that this was a violation of company policy. I found Applicant's testimony to be elusive, at times evasive, and utterly unconvincing. He failed to produce sufficient evidence to counter the testimony of the government's witness and the company's records. In testimony, Applicant also admitted to, and then denied, improperly entering a SCIF without "badging in" as required. Although this was not alleged in the SOR and will not be considered for disqualifying purposes, it may be considered when making a credibility determination, in the application of mitigating conditions, and in my whole-person analysis.

Based on the totality of the allegations and recurring inappropriate conduct, Applicant's judgment continues to be questionable. He has not submitted sufficient evidence to alleviate those concerns. The allegations are not minor, nor did they occur in unique circumstances where they are not likely to recur. He has not accepted full responsibility for his conduct, and failed to show sufficient mitigating evidence. I find no mitigating condition is fully applicable.

**Guideline M: Use of Information Technology**

AG ¶ 39 expresses the security concern pertaining to use of information technology systems:

> Failure to comply with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns

about an individual's reliably and trustworthiness, calling into question the willingness or ability to properly protect sensitive systems, networks, and information. Information Technology Systems 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 describes conditions that could raise a security concern and may be disqualifying. I considered the following relevant:

(e) unauthorized use of any information technology system.

Applicant wrongly permitted his girlfriend to certify his timecard on his behalf, a violation of company policy. AG ¶ 40(e) applies.

I have considered all of the mitigating conditions under AG ¶ 41 and considered the following relevant:

(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.

Applicant's conduct was intentional, recent, and recurring. He was trained and understood how to use the timekeeping system. He showed poor judgment and was terminated for violations of the company and security policies. Applicant admitted to improperly allowing his girlfriend to certify his timecard, but attempted to justify his actions based on his medical condition at the time. This incident alone may be mitigated by time or otherwise minor, but overall, I find Applicant's response to the allegations to be evasive, unrepentant, and unconvincing. He did not submit sufficient evidence to refute the Government's allegations, and I am convinced his improper use of the timecard system was knowing and intentional. No mitigating condition fully applies.

## Whole-Person Concept

Under AG ¶¶ 2(a), 2(c), and 2(d), the ultimate determination of whether to grant national security eligibility must be an overall commonsense judgment based upon careful consideration of the guidelines and the 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).

I considered all of the potentially disqualifying and mitigating conditions in light of all the facts and circumstances surrounding this case. I have incorporated my findings of fact and comments under Guidelines E and M in my whole-person analysis.

Applicant has not taken convincing steps to acknowledge his behavior and the impact it had on his company and the government client. He did not present sufficient mitigating evidence or convincingly refute the Government's allegations. Accordingly, I conclude he has not carried his burden of showing that it is clearly consistent with the national security interests of the United States to grant or continue eligibility for access to classified information.

## 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

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

_____
Gregg A. Cervi
Administrative Judge