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

| | | |
|---|---|---|
| In the matter of: | ) | |
| | ) | |
| | ) | ISCR Case No. 17-02612 |
| | ) | |
| | ) | |
| Applicant for Security Clearance | ) | |

## Appearances

For Government: Tara Karoian, Esq., Department Counsel
For Applicant: *Pro se*

February 11, 2019

_____

## Decision

_____

CEFOLA, Richard A., Administrative Judge:

## Statement of the Case

On December 1, 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 E, M, and K. 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.

Applicant answered the SOR on December 14, 2017, and requested a hearing before an administrative judge. (Answer.) The case was assigned to me on February 6, 2018. The Defense Office of Hearings and Appeals (DOHA) issued a notice of hearing on February 12, 2018, scheduling the hearing for March 20, 2018. The hearing was convened as scheduled. The Government offered Exhibits (GX) 1 through 3, which were admitted without objection. Applicant testified on his own behalf and presented two sets of documents, which I marked Applicant's Exhibits (AppXs) A and B, and admitted into evidence. The record was left open until April 17, 2018, for receipt of additional

documentation. On April 17, 2018, Applicant offered AppX C, which was also admitted into evidence. DOHA received the transcript of the hearing (TR) on March 28, 2018.

## Findings of Fact

Applicant admitted to the allegations in SOR ¶¶ 2.a., and 2.b. He denied SOR allegations ¶¶ 1.a., and 3.a. After a thorough and careful review of the pleadings, exhibits, and testimony, I make the following findings of fact.

Applicant is a 41-year-old employee of a defense contractor. (TR at page 18 line 23 to page 19 line 9, and GX 1 at page 5.) He has been employed with the defense contractor since "April of" 2017. (GX 1 at page 5.) Applicant was terminated by his prior employer in September of 2015 for "Policy Violations," that will be discussed at length, below. (GX 3.) He served in the Marine Corp from 2000~2006, achieving the rank of Sergeant. (AppX C at page 3.)

**Guideline M - Use of Information Technology, Guideline K - Handling Protected Information & Guideline E - Personal Conduct**

1.a., 2.a. and 2.b. Applicant admits that at his prior employment he installed unauthorized software, a Mouse Jiggler," which prevented his "screen from locking out." (TR at page 24 line 23 to page 31 line 6.) He avers that he was "unaware that it was unauthorized," as he was introduced to it "by a senior administrator that(*sic*) was acting as a mentor to . . . [Applicant] at that time." (*Id*, and TR at page 84 lines 4~17.) Applicant has offered five undated letters of support from those he works with at his current employer, but nothing to corroborate averment regarding the unauthorized software.

1.a., and 3.a. Applicant denies that he created five administrated accounts, some in the names of coworkers, on a classified system without approval. (TR at page 31 line 7 to page 45 line 8, at pages 50 line 15 to page 51 line 3, and at page 55 line 11 to page 68 line 5.) He avers this misconduct was authorized. (TR at page 83 line 25 to page 84 line 3.) However, Applicant has submitted nothing further in support of his averment.

1.a. Applicant denies that he falsified his time card over a seven day period. (TR at page 45 line 19 to page 50 line 14.) His "Desktop' was monitored by his employer for seven of a planned ten days. (AppX A at page 1.) During this period, Applicant "spent" the majority of his "**Active Time** on **Non-Work** related activities . . . included doing homework, browsing online retailers, and watching YouTube videos." (*Id*.) I find that this was a clear misuse of information technology.

## Policies

When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the adjudicative guidelines (AG). In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially disqualifying conditions and mitigating conditions, which are useful 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, administrative judges apply the guidelines 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. According to AG ¶ 2(a), 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. 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 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 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 information.

Section 7 of Executive Order 10865 provides that adverse 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 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. Two are potentially applicable in this case:

(e) unauthorized use of any information technology system; and

(f) introduction, removal, or duplication of hardware, firmware, software, or media to or from any information technology system when prohibited by rules, procedures, guidelines, or regulations or when otherwise not authorized

Applicant downloaded an unauthorized Mouse Jiggler on his employer's laptop. This conduct is sufficient to raise the above disqualifying conditions.

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.

None of these apply. This deliberate manipulation of his employer's information technology system was intentional, not authorized, and occurred only about two and a half years prior to his hearing. Guideline M is found against Applicant.

**Guideline K - Handling Protected Information**

The security concern relating to the guideline for Handling Protected Information is set out in AG ¶ 33:

> Deliberate or negligent failure to comply with rules and regulations for handling protected information-which includes classified and other sensitive government information, and proprietary information-raises doubt about an individual's trustworthiness, judgment, reliability, or willingness and ability to safeguard such information, and is a serious security concern.

The guideline notes several conditions that could raise security concerns under AG ¶ 34. One is potentially applicable in this case:

> (g) any failure to comply with rules for the protection of classified or sensitive information.

Applicant created five administrative accounts in the names of colleagues on his classified system without approval. This conduct is sufficient to raise the above disqualifying condition.

AG ¶ 35 provides conditions that could mitigate security concerns. I considered all of the mitigating conditions under AG ¶ 35 including:

> (a) so much time has elapsed since the behavior, or it has happened so infrequently or 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 individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities;
>
> (c) the security violations were due to improper or inadequate training or unclear instructions; and
>
> (d) the violation was inadvertent, it was promptly reported, there is no evidence of compromise, and it does not suggest a pattern.

Again, none of these apply. Although his misconduct occurred more than two years ago; I can't overlook the fact that it was deliberate and intentional, and Applicant shows no remorse for said conduct. Guideline K is found against Applicant.

**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.

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

> (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;

Applicant has a demonstrated pattern of rule violations. The evidence is sufficient to raise these disqualifying conditions.

AG ¶ 17 provides conditions that could mitigate security concerns. I considered all of the mitigating conditions under AG ¶ 17 including:

> (a) the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts;
>
> (b) the refusal or failure to cooperate, omission, or concealment was caused or significantly contributed to by advice of legal counsel or of a person with professional responsibilities for advising or instructing the individual specifically concerning security processes. Upon being made

aware of the requirement to cooperate or provide the information, the individual cooperated fully and truthfully;

(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;

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

(f) the information was unsubstantiated or from a source of questionable reliability; and

(g) association with persons involved in criminal activities was unwitting, has ceased, or occurs under circumstances that do not cast doubt upon the individual's reliability, trustworthiness, judgment, or willingness to comply with rules and regulations.

None of these apply. Applicant falsified his time cards, downloaded unauthorized software, and created unauthorized administrative accounts. What is most troubling is that Applicant shows little or no remorse for his Personal Conduct. Guideline E is found against Applicant.

**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 national security eligibility 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, K, and E in my whole-person analysis. Applicant is well respected with his current employer. (AppX C.) However given his pattern of rule violations, overall, the record evidence leaves me with questions and doubts as to Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude Applicant mitigated/failed to mitigate the Use of Information Technology, Handling Protected Information, and Personal Conduct security 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 E: | AGAINST APPLICANT |
| Subparagraph 1.a: | Against Applicant |
| Paragraph 2, Guideline M: | AGAINST APPLICANT |
| Subparagraph 2.a: | Against Applicant |
| Subparagraph 2.b: | Against Applicant |
| Paragraph 3, Guideline K: | AGAINST APPLICANT |
| Subparagraph 3.a: | 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 interest to grant Applicant eligibility for a security clearance. National security eligibility for access to classified information is denied.

_____
Richard A. Cefola
Administrative Judge