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

| | | |
|---|---|---|
| In the matter of: | ) | |
| | ) | |
| | ) | ISCR Case No. 15-05232 |
| | ) | |
| Applicant for Security Clearance | ) | |

## Appearances

For Government: Ross Hyams, Esq., Department Counsel
For Applicant: *Pro se*

01/24/2018

## Decision

CERVI, Gregg A., Administrative Judge

This case involves security concerns raised under Guideline E (Personal Conduct), Guideline D (Sexual Behavior), 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 July 18, 2014. On August 31, 2016, the Department of Defense Consolidated Adjudications Facility (DOD CAF) sent him a Statement of Reasons (SOR) alleging security concerns under Guidelines E, D, and M.[1]

Applicant responded to the SOR on September 29, 2016, and requested a hearing before an administrative judge. The Defense Office of Hearings and Appeals issued a

[1] The DOD 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) implemented by the DOD on September 1, 2006.

notice of hearing on March 8, 2017, and the hearing was convened on April 3, 2017. Government Exhibits (GE) 1 through 5 were admitted in evidence. Applicant testified and submitted Applicant's Exhibit (AE) A, which was admitted. DOHA received the hearing transcript (Tr.) on April 12, 2017.

## Findings of Fact

Applicant is a 53-year-old computer operator, currently employed by a government agency since June 2016, and sponsored for a security clearance by a defense contractor. He previously worked for a defense contractor from June 2013 until he was terminated in February 2014 for violating company and government policies. He received a bachelor's degree in 2009 and is working toward a master's degree. He married in 1987 and separated in 2014. He has three children. He retired from the U.S. Air Force in 2012 after a 24-year career. He previously held a DOD security clearance that was revoked in 2010 and never reinstated. He also holds a public trust position.

The SOR alleges under Guideline E, that Applicant violated company and government computer policies in 2013 by installing extrapolation software on a government issued computer to obtain a product key for use without a license, for bypassing login procedures, and for accessing pornographic images from 1995 to 1996 and in 2013. These allegations were cross-alleged under Guidelines D and M. In addition, Applicant is alleged under Guideline D to have installed a hidden camera in their bedroom to view his wife without her knowledge; to have been diagnosed with a partner relational problem and impulse control disorder not otherwise specified; and exhibiting a pattern of compulsiveness in viewing pornography. Applicant generally admitted the SOR allegations, but disputed bypassing login procedures and viewing pornographic directly from pornographic websites with his government computer. He provided explanations and clarifications in his answer to the SOR.

In 2003, while stationed overseas on active duty, Applicant installed a hidden camera in his home bathroom, connected to a television in his bedroom, to surreptitiously view his spouse without her consent. She discovered the camera after about two weeks of operation, and reported the incident to military authorities. No charges were preferred because his spouse refused to cooperate, but his access to sensitive compartmented information (SCI) was revoked. As a result of this incident, Applicant began life skills counseling and was diagnosed with impulse control disorder not otherwise specified. He attended weekly addiction counseling group sessions (12-step program) through his church and at military mental health facilities, and he and his spouse attended marital therapy. As a result of viewing pornography on a government computer, which resulted in a letter of reprimand, and hiding pornographic viewing from his spouse on his home computer while also surreptitiously viewing her in the bathroom without her consent, Applicant's security clearance was finally revoked in 2010 under guidelines for sexual behavior, psychological conditions, and use of information technology systems.

In 2014, Applicant was terminated from employment with a defense contractor for violation of company and government computer-use policies. He was found to have

accessed inappropriate materials via the internet; downloaded inappropriate material to the hard drive; downloaded unauthorized software from the internet; connected an unauthorized external device to his government computer to watch pirated movies; and performed a Google facial recognition search that resulted in inappropriate content. In 2014, Applicant was confronted with these violations and he concurred in the allegations in the report. He was terminated in February 2014.

Applicant stated that extrapolating a product key to use without a license was in furtherance of work efficiency, and that inappropriate images were imbedded in gaming sites he visited, not by intentionally accessing pornography. However in his testimony, he noted his difficulty with viewing inappropriate images on computers, which resulted in his termination. He stated he was going through a "rough patch" in his marriage, and noted his regular attendance at addiction counseling from 2009 to 2014.

Applicant submitted a favorable character reference letter, dated April 2010, from a professor and retired government scientist that facilitates a church-sponsored pornography addiction support group that Applicant attended.

## Policies

The Director of National Intelligence (DNI) issued revised adjudicative guidelines (AG) in a Security Executive Agent Directive, on June 8, 2017. The revised guidelines are applicable to this decision.

"[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. See 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 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. See 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;

(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:

. . .

(2) any disruptive, violent, or other inappropriate behavior . . . .

(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, may affect the person's personal, professional, or community standing.

Applicant's conduct as noted in the findings of fact, invokes an assessment of questionable judgment and personal conduct that creates a vulnerability to exploitation, manipulation, or duress. AG ¶¶ 16(c), (d), and (e) 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 behavior, taken as a whole, shows a pattern of unmitigated misconduct, including repeated incidents of wrongful use of company and government technology, and inappropriate personal conduct in surreptitiously viewing his spouse without her consent. Based on the totality of the allegations and recurring inappropriate conduct up to 2013, 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. Although he has undertaken counseling over a number of years, his inappropriate behavior continued unabated. He has not taken sufficient steps to remediate his behavior, or eliminate the vulnerabilities that it creates. I find no mitigating condition is fully applicable.

**Guideline D: Sexual Behavior**

AG ¶ 12 expresses the security concern:

> Sexual behavior that involves a criminal offense; reflects a lack of judgment or discretion; or may subject the individual to undue influence of coercion, exploitation, or duress. These issues, together or individually, may raise questions about an individual's judgment, reliability, trustworthiness, and ability to protect classified or sensitive information. Sexual behavior includes conduct occurring in person or via audio, visual, electronic, or written transmission.

AG ¶ 13 describes conditions that could raise a security concern and may be disqualifying. The following condition may be applicable:

> (a) sexual behavior of a criminal nature, whether or not the individual has been prosecuted;
>
> (b) a pattern of compulsive, self-destructive, or high-risk sexual behavior that the individual is unable to stop;
>
> (c) sexual behavior that causes an individual to be vulnerable to coercion, exploitation, or duress; and
>
> (d) sexual behavior of a public nature or that reflects lack of discretion or judgment.

Applicant's misconduct, including surreptitiously viewing his spouse in the bathroom without consent and accessing inappropriate material on government or company computers, sufficiently raise the disqualifying conditions above. SOR ¶ 2.b does not implicate sexual behavior as contemplated by this guideline, but may be considered in evaluating his conduct under this and other guidelines. SOR ¶ 2.b is resolved in Applicant's favor.

AG ¶ 14 provides conditions that could mitigate security concerns. I reviewed the facts against all of the mitigating conditions. I find that the following mitigating conditions potentially apply:

> (b) the sexual behavior happened so long ago, 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; and
>
> (c) the behavior no longer serves as a basis for coercion, exploitation, or duress.

I find no mitigating condition fully applies. Applicant's actions with regard to the SOR allegations involve repeated inappropriate conduct that continue to reflect a lack of good judgment and a pattern of inappropriate sexual behavior. The occurrences were frequent, happened under normal circumstances, and continued despite its discovery, past disciplinary and security clearance action, and counseling. Applicant has not taken sufficient responsibility for his actions or submitted sufficient or recent psychological treatment records to mitigate the behavior. I find no reason to believe that Applicant's conduct has permanently ceased or that it will not occur again in the future.

**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:

> (a) unauthorized entry into any information technology system;
>
> (b) unauthorized modification, destruction, or manipulation of, or denial of access to, an information technology system or any data in such a system;
>
> (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 regulation or when otherwise not authorized.

Applicant installed extrapolation software to obtain a product key without a license, accessed unauthorized websites, and viewed inappropriate material on government computers in violation of government and company policies. AG ¶¶ 40(a), (b), (e), and (f) apply.

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; and

(b) the misuse was minor and done solely in the interest of organizational efficiency and effectiveness.

Applicant's conduct was intentional, recent, and recurring. Although he claims to have attempted to access the product key in furtherance of work efficiency, his actions were unauthorized. His recurring computer misconduct show a degree of unreliability, untrustworthiness, and bad judgment. Additionally, insufficient time has passed to determine whether he has truly learned from these incidents and modified his behavior. AG ¶¶ 41(a) and (b) do not apply.

**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, D, and M in my whole-person analysis.

Applicant has not shown that he can be trusted with company or government computer access, and has a history of inappropriate sexual conduct and misuse of information technology. His actions have not been appropriately mitigated by counseling or psychological treatment, and he has not shown that continued misconduct will not

occur in the future. 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 him eligibility for access to classified information.[2]

## 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 |
| Subparagraphs 1.a – 1.c: | Against Applicant |
| Paragraph 2, Guideline D: | Against Applicant |
| Subparagraphs 2.a and 2.c: | Against Applicant |
| Subparagraph 2.b: | For Applicant |
| Paragraph 3, Guideline M: | Against Applicant |
| Subparagraph 3.a: | Against Applicant |

## Conclusion

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

_____
Gregg A. Cervi
Administrative Judge

[2] No exceptions under Security Executive Agent Directive (SEAD) 4, Appendix C, are applicable.