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

| | | |
|---|---|---|
| In the matter of: | ) | |
| | ) | |
| XXXXXXXXXX, XXXXX | ) | ISCR Case No. 14-00212 |
| | ) | |
| Applicant for Security Clearance | ) | |

## Appearances

For Government: Chris Morin, Esq., Department Counsel
For Applicant: Alan V. Edmunds, Esq.

09/23/2014

## Decision

TUIDER, Robert J., Administrative Judge:

Use of information technology systems, handling protected information, and personal conduct security concerns were identified after Applicant left the employment of a defense contractor and began working for a competitor defense contractor. Applicant successfully mitigated those concerns. Eligibility for access to classified information is granted.

## Statement of the Case

On August 27, 2012, Applicant submitted an Electronic Questionnaire for Investigations Processing (e-QIP) or security clearance application (SF 86). On March 20, 2014, the Department of Defense (DOD) Consolidated Adjudications Facility (CAF) issued an SOR to Applicant, pursuant to Executive Order 10865, *Safeguarding Classified Information Within Industry,* dated February 20, 1960, as amended; DOD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (Directive), dated January 2, 1992, as amended; and the adjudicative guidelines (AG) promulgated by the President on December 29, 2005.

The SOR alleged security concerns under Guidelines M (use of Information technology systems), K (handling protected information), and E (personal conduct). The SOR detailed reasons why the DOD CAF was unable to find that it is clearly

consistent with the national interest to continue a security clearance for Applicant, and it recommended that his case be submitted to an administrative judge for a determination whether his clearance should be continued or revoked.

On May 2, 2014, Applicant responded to the SOR. On July 14, 2014, Department Counsel was ready to proceed on Applicant's case. On July 18, 2014, DOHA assigned Applicant's case to me. On July 30, 2014, the Defense Office of Hearings and Appeals (DOHA) issued a hearing notice, setting the hearing for August 25, 2014. Applicant's hearing was held as scheduled. At the hearing, Department Counsel offered Government Exhibits (GE) 1 through 4 and Hearing Exhibit (HE) I, which were received into evidence without objection. Applicant called three witnesses, testified, and offered Applicant Exhibits (AE) A through H, which were received into evidence without objection.

I held the record open until September 15, 2014, to afford the Applicant the opportunity to submit additional documents. Applicant timely submitted AE I and AE J, which was received into evidence without objection. On September 4, 2014, DOHA received the hearing transcript (Tr.).

## Findings of Fact[1]

In his Answer to the SOR, Applicant admitted in part the SOR allegations with explanations. Applicant's admissions and explanations are incorporated as findings of fact.

### Background Information

Applicant is a 38-year-old senior software engineer, who has been employed by a defense contractor since June 2012. He seeks to retain his secret security clearance, which is a condition of his continued employment. Applicant has held a secret security clearance since 2008. (Tr. 35-37, 65-67, GE 1.)

Applicant was awarded a bachelor of science degree in aerospace engineering in May 1998, and a master's degree in software engineering in May 2000. (Tr. 36, 66-67, GE 1.) He married in February 1999, and has five minor children. Applicant's wife does not work outside the home. (Tr. 35, 65-66, GE1.) He has not served in the armed forces. (Tr. 35, GE 1.)

### Use of Information Technology Systems/Handling Protected Information/Personal Conduct

The facts of this case involve Applicant's purported misuse of information technology, his purported failure to protect sensitive information, and the misrepresentation of his conduct surrounding these events. Applicant was previously

[1]Some details have been excluded in order to protect Applicant's right to privacy. Specific information is available in the cited exhibits.

employed by defense contractor (DCA) from June 2008 to June 2012 as a senior staff software engineer until he began his current employment with defense contractor (DCB) in June 2012 as a senior software engineer. DCA and DCB are competitor defense contractors. (Tr. 36-38, GE 1.) It is not disputed that in May 2012 before leaving DCA, Applicant copied DCA proprietary data from his DCA computer workstation to an external hard drive belonging to DCA. He took the DCA external hard drive home and then copied and/or downloaded data files to his personal computer. (Tr. 36-39, 58-63, SOR answer.)

Applicant disputes the allegation that he accessed the external hard drive remotely from home or that he transmitted sensitive data over a network from a remote location, or that he failed to safeguard the data from his workstation to his home computer and back. He cited a past example of how DCA allowed him to take his entire workstation home following a major storm. He further disputes that he remotely accessed data from home suggesting that he copied sensitive data over an unsecure network. He stated that he copied the data to an external hard drive, that he copied the data to his home computer, and returned the drive to DCA. Applicant asserted that it was customary for DCA to allow employees to take data home so that he could work at home. His purpose in taking the work home was to complete DCA tasks. Applicant's testimony was credible and not rebutted.[2] (Tr. 39-40, 60-65, SOR answer.)

More problematic for Applicant, however, are integrity allegations. On June 27, 2012, after Applicant began working for DCB, he was summoned to the DCB corporate offices and was queried by DCB's General Counsel (GC) whether he had DCA data at his home. He denied that he did, which was not true. Recognizing that he had not been truthful and after consulting his pastor, Applicant sent a letter dated July 6, 2012 to DCA's GC, copying DCB's GC and senior vice-president, advising that he had not been truthful during his June 27, 2012 DCB GC interview.[3] He discussed his failure to follow protocol and characterized his impromptu answers as "a disheartening act of self-preservation over full disclosure and honesty." Applicant recognized at the time that he submitted his July 6, 2012 letter that he was exposing himself to adverse action to include losing his job with DCB. (Tr. 40-61, SOR answer, GE 2, GE 3, GE 4, AE A.)

Also problematic for Applicant is an allegation that during his DCA May 31, 2012 exit interview, approximately nine days before his last day at DCA, he stated that he had not retained any DCA confidential or proprietary information. At the time of his exit interview Applicant advised the human resource manager (HRM) that he had files at home that he was working on. The HRM directed him to check the block indicating that he had not retained any DCA data because she would not be in her office on his last

[2] Applicant's testimony was corroborated in the form of a DCB GC June 2012 letter to DCA's GC, particularly as it pertains to his purported failure to safeguard DCA sensitive data from DCB's GC and the fact that he was allowed to work on DCA projects at home as he did. (GE 2.)

[3] Shortly after Applicant's July 6, 2012 letter, DCA filed a lawsuit against him. The lawsuit was settled on September 25, 2012. Under the terms agreed upon, he is prohibited from discussing settlement terms. (Tr. 50-51.) Applicant remains a DCB employee in good standing.

day of work, June 8, 2012. Applicant's testimony was credible and not rebutted. (SOR answer.)

**Character Evidence**

Applicant called three credible character witnesses to testify on his behalf. These witnesses have been associated with Applicant on a professional basis, have security clearances, and are familiar with the requirements of holding a security clearance. In spite of the SOR allegations, the witnesses remained steadfast in their support of Applicant. The witnesses emphasized Applicant's work ethic, good character, and trustworthiness. (Tr. 17-34.) Additionally, Applicant submitted three work-related reference letters that echoed the witnesses' favorable testimony. The reference letters also discussed the significant contribution Applicant makes in support of the national defense. (AE D - AE F.) Lastly, Applicant submitted two awards he received at DCA, his most recent DCB performance evaluation (2/2/13 – 1/31/14), and a DCB merit pay increase and promotion. His performance rating was favorable enough to warrant a salary increase. (AE G – AE J.)

## Policies

The U.S. Supreme Court has recognized the substantial discretion of the Executive Branch in regulating access to information pertaining to national security emphasizing, "no 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 applicant's 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, *Safeguarding Classified Information within Industry* § 2 (Feb. 20, 1960), as amended.

Eligibility for a security clearance 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, these guidelines are applied 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, 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 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 "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." *See* Exec. Or. 10865 § 7.

*See also* Executive Order 12968 (Aug. 2, 1995), § 3.1. Thus, nothing in this Decision should be construed to suggest that I have based this decision, in whole or in part, on any express or implied determination about applicant's allegiance, loyalty, or patriotism. It 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. 95-0611 at 2 (App. Bd. May 2, 1996).

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 ultimate burden of demonstrating that it is clearly consistent with the national interest to grant or continue his or her security clearance." ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002). The burden of disproving a mitigating condition never shifts to the Government. *See* ISCR Case No. 02-31154 at 5 (App. Bd. Sep. 22, 2005). "[S]ecurity clearance determinations should err, if they must, on the side of denials." *Egan*, 484 U.S. at 531; *see* AG ¶ 2(b).

## Analysis

### Use of Information Technology Systems

AG ¶ 39 articulates the security concern relating to use of information technology systems:

> Noncompliance 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 Systems include all related computer hardware, software, manipulation, storage, or protection of information.

Potentially disqualifying conditions under this concern are: AG ¶ 40(c) "use of any information technology system to gain unauthorized access to another system or to a compartmented area within the same system;" AG ¶ 40(f) "introduction, removal, or duplication of hardware, firmware, software, or media to or from any information technology system without authorization, when prohibited by rules, procedures, guidelines, or regulations;" and AG ¶ 40(g) "negligence or lax security habits in handling information technology that persist despite counseling by management."

There are three mitigation conditions under this guideline that potentially apply: 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;" AG ¶ 41(b) "the misuse was minor and done only in the interest of organizational efficiency and effectiveness, such as letting another person use one's password or computer when no other timely alternative was readily available;" and AG ¶ 41(c) "the conduct was unintentional or inadvertent and was followed by a prompt, good faith effort to correct the situation and by notification of a supervisor."

Applicant took work home to ensure that he completed a DCA project before he left their employment. Although he did not specifically request permission to do so in this particular case, Applicant submitted sufficient evidence to establish that taking work home in the manner that he did was common practice. A similar situation is unlikely to reoccur. It also became clear that Applicant's motivation for taking work home was to complete his work before leaving DCA and not for any other reason. Applicant notified DCA's HRM during his exit interview that he was working on DCA files at home; however, she directed him to check the box that he did not have any DCA files in his possession because she was not going to be in the office on the last day of his employment. Mitigating conditions AG ¶¶ 41(a), 41(b), and 41(c) are applicable.

**Handling Protected Information**

AG ¶ 33 articulates the security concern relating to handling protected information:

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

Potentially disqualifying conditions under this concern are: AG ¶ 34(b) "collecting or storing classified or other protected information at home or in any other authorized location;" and AG ¶ 34(g) "any failure to comply with rules for the protection of classified or other sensitive information."

There are three mitigation conditions under this guideline that potentially apply: AG ¶ 35(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;" AG ¶ 35(b) "the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge or security responsibilities;" and AG ¶ AG 35(c) "the security violations were due to improper or inadequate training."

The discussion under Use of Information Technology Systems is applicable under this section. Applicant has assimilated well into his new position with DCB and has received security training consistent with his responsibilities. His witnesses and

character references made it clear that he demonstrates a positive attitude towards his security responsibilities. Whatever security training DCA may have given Applicant was undermined by the informal practices condoned by management to get the job done. Applicant cited examples of having taken work home to include propriety data on several occasions without consequences while a DCA employee. Mitigating conditions AG ¶¶ 34(a), 35(b), and 35(c) are applicable.

**Personal Conduct**

AG ¶ 15 articulates the security concern relating to personal conduct:

> 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 information. Of special interest is any failure to provide truthful and candid answers during the security clearance process or any other failure to cooperate with the security clearance process.

A potentially disqualifying condition under this concern is: AG ¶ 16(b) "deliberately providing false or misleading information concerning relevant facts to any employer, investigator, security official, competent medical authority, or other government representative."

There are three mitigation conditions under this guideline that potentially apply: AG ¶ 17(a) "the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts;" 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;" and 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 caused untrustworthy, unreliable, or other inappropriate behavior, and such behavior is unlikely to recur."

The discussion under Use of Information Technology Systems and Handling Protected Information is applicable under this section. Ten days after Applicant lied to DCB's GC regarding DCA data, he "came clean" and wrote a letter to DCA's GC with a copy to DCB's GC and senior vice-president admitting his misrepresentation. The fact that he was the sole income earner supporting a wife and five minor children is not lost on me. Applicant put his career and ability to support his family in jeopardy. This process was clearly a painful lesson for Applicant. His purported May 31, 2012 misrepresentation during his DCA exit interview is mitigated by the fact that he informed the DCA HRM that he had DCA data at home. Furthermore, Applicant was using the DCA data to complete his project before he left DCA's employment and such was an accepted DCA practice at that time. Mitigating conditions AG ¶¶ 17(a), 17(d), and 17(d) are applicable.

## 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 the circumstances. The administrative judge should consider the nine adjudicative process factors listed at AG ¶ 2(a):

> (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.

The ultimate determination of whether to grant eligibility for a security clearance must be an overall commonsense judgment based upon careful consideration of the guidelines and the whole-person concept. AG ¶ 2(c). I have incorporated my comments under Guidelines M, K, and E in my whole-person analysis. Some of the factors in AG ¶ 2(a) were addressed under those guidelines, but some warrant additional comment.

Applicant is a 38-year-old senior software engineer, who has worked for his employer since 2012 and has held a security clearance since 2008. He is sufficiently mature to understand and comply with his security responsibilities. There is every indication that he is loyal to the United States and his employer. The most serious allegation Applicant faced are the integrity issues surrounding his June 2012 interview with DCB's GC. He was able to overcome his lapse in judgment by the subsequent corrective action he took. It was no small undertaking for Applicant to "come clean" to put in writing that he had lied knowing that he would run the risk of being professionally ruined and putting his family's future at risk. I am satisfied that Applicant recognizes the Government's concerns in this case. The unique circumstances that led to these security concerns are unlikely to occur again. However, if such circumstances ever did arise again, I am confident that Applicant would not make the same mistake again.

Lastly, Applicant's character letters and witness testimony attest to his good character for trustworthiness, diligence, responsibility, and conscientious, detail-oriented contributions to his employer and community. He is a valued employee who is making a contribution to the national defense, a dedicated family man, and contributing member of society. It is also apparent that this process made a significant and lasting impression on the Applicant.

I have carefully applied the law, as set forth in *Department of Navy v. Egan,* 484 U.S. 518 (1988), Exec. Or. 10865, the Directive, and the AGs, to the facts and circumstances in the context of the whole-person. I conclude handling protected information, use of information technology systems, and personal conduct concerns are mitigated, and eligibility for access to classified information is granted.

## 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 M: | FOR APPLICANT |
| Subparagraph 1.a: | For Applicant |
| Paragraph 2: Guideline K: | FOR APPLICANT |
| Subparagraph 2.a: | For Applicant |
| Paragraph 3: Guideline E: | FOR APPLICANT |
| Subparagraphs 3.a – 3.c: | For Applicant |

## Conclusion

In light of all the circumstances presented by the record in this case, it is clearly consistent with the national interest to grant Applicant's eligibility for a security clearance. Eligibility for a security clearance is granted.

_____
Robert J. Tuider
Administrative Judge