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

| | | |
|---|---|---|
| In the matter of: | ) | |
| | ) | |
| | ) | ISCR Case No. 14-00963 |
| | ) | |
| Applicant for Security Clearance | ) | |

## Appearances

For Government: Christopher Morin, Esq., Department Counsel
For Applicant: *Pro se*

10/10/2014

## Decision

DUFFY, James F., Administrative Judge:

Applicant failed to mitigate security concerns arising under Guideline K (Handling Protected Information), and Guideline M (Use of Information Technology Systems). Clearance is denied.

## Statement of the Case

On April 28, 2014, the Department of Defense Consolidated Adjudications Facility (DOD CAF) issued Applicant a Statement of Reasons (SOR) detailing security concerns under Guidelines K and M. This action was taken under Executive Order 10865, *Safeguarding Classified Information Within Industry,* dated February 20, 1960, as amended; Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program,* dated January 2, 1992, as amended (Directive); and the adjudicative guidelines (AG) implemented on September 1, 2006.

The SOR detailed reasons why DOD CAF could not find under the Directive that it is clearly consistent with the national interest to grant or continue Applicant's security clearance. On May 16, 2014, Applicant answered the SOR and requested a hearing.

The case was assigned to me on July 15, 2014. DOHA issued the Notice of Hearing on July 24, 2014. The hearing was held as scheduled on August 12, 2014.

At the hearing, Department Counsel offered Government Exhibits (GE) 1 through 3, while Applicant testified and offered Applicant Exhibits (AE) A though I. All proffered exhibits were admitted into evidence without objection. The prehearing guidance sent to Applicant was marked as Hearing Exhibit (HE) 1 and Department Counsel's list of exhibits was marked as HE 2. The transcript (Tr.) of the hearing was received on August 21, 2014.

## Findings of Fact

Applicant is a 52-year-old technical drafter who works for a defense contractor. He has been working for his current employer since about November 2011. He graduated from high school in 1980 and completed about two years of technical school. He has been married twice. His first marriage was from 1984 to 1993. He married his current wife in 1999. He has two children, ages 32 and 15. He held a security clearance from about 1982 to 2011 without incident.[1]

The SOR alleged under Guideline K that Applicant obtained access by an unauthorized means to a company's proprietary information, official government documentation, a cleared facility floor plan, and sensitive company financial data in October 2011, and that he improperly stored that information on an external hard drive that belonged to the company. The sole Guideline K allegation was cross-alleged as a single allegation under Guideline M. In his Answer to the SOR, Applicant admitted both allegations with comments. Those comments are interpreted and treated as denials of the allegations.[2]

From 1982 to 2011, Applicant worked for a company [hereafter referred to as "Company A"]. In that job, his duties included conducting site surveys and drafting floor plans for classified areas such as command centers. The company's clients included DOD components as well as DOD contractors. Throughout the years, he signed nondisclosure agreements and knew he was obligated to protect the company's proprietary information.[3]

[1] Tr. 5-8, 36-37; GE 1; AE A.

[2] Applicant's Answer to the SOR.

[3] Tr. 37-40. During cross-examination, Applicant was asked whether he signed a nondisclosure agreement and he testified as follows:

> [Department Counsel]: And do you recall signing a nondisclosure agreement which provided that you wouldn't share any of your work product or any of [Company A's] information with others unless you were authorized to do so by [Company A].
>
> [Applicant]: I know we had – I don't remember it, but yes, I know that we had different documents through the years.

While working at Company A, Applicant would routinely backup computer data to a company external hard drive. The company did not have an automatic backup system on their computers. The external hard drive was about the size of a person's fist and contained proprietary data and financial information from Company A as well as Government drawings. It did not contain classified information. As part of his supervisory responsibilities, he also ensured subordinates backed up their work data on computers. He frequently carried the external hard drive home after work.[4]

In the fall of 2011, Applicant decided to leave Company A so that he could begin working for a competitor, Company B. At that time, the workload at Company A was decreasing, and he was concerned the company would start laying off employees. He also thought that Company B would be a less stressful place to work. One of his former supervisors and about 15 other individuals had already left Company A and were then working for Company B. Applicant's former supervisor recruited him for this new job. Once an employee of Company A gave his or her two-week notice of leaving, the employee was not allowed to continue working there and was immediately released.[5]

In an Office of Personnel Management (OPM) interview, Applicant reportedly stated:

> The week/days before [Applicant] resigned from [Company A] [Applicant] transferred/copied all of the projects that he worked on just for his own personal reference. [Applicant's] work with [Company B] is the same work he did at [Company A] and [Applicant] copied the files/folders for examples to help him reference his work. [Applicant] did not copy the files to harm or bid against [Company A] and he [had] no bad intentions when he was copying these files. [Applicant] was not aware that he doing anything wrong and the only reason why he copied the files/transferred the files was to reference his work and he did not transfer the files to take any of [Company A's] clients/work/bids or business.[6]

---

> [Department Counsel]: Well, did you understand that when you were at [Company A] that you couldn't share their proprietary information or information that they through contracting and work for other clients –
>
> [Applicant]: We weren't able to just give anything away, yes.

In his Answer, Applicant stated: "I do understand protecting government and company information. I don't just give out drawings to other companies. I know the rules and when other folks just blindly e-mail or call me asking for files, I went thru the proper [Government] chain of command and have gotten permission to forward or NOT to forward information to the inquiring parties."

[4] Tr. 38-39, 43-48.

[5] Tr. 39-43.

[6] Tr. 21-25, 43-48; GE 2.

In his Answer to the SOR, Applicant stated:

> I did wait until 4:00 on the day I gave my notice and there was only a handful of folks left, I did back up my work to the orange hard drive that was owned by [Company A]. I cried my eyes out as I was walking out; I packed up the [Company A] hard drive without thinking during this emotional period. EVERYONE who gave a notice that [he or she] was leaving to another company was immediately forced to pack their belongings and exit the property ASAP. I didn't want to be treated as a criminal and forced to walk out, so I pre packed and DELIBERATED and cried in my private office right up to the very last second. I had 30 Xerox boxes in my garage and that hard drive got tossed into one of them.[7]

In his testimony, Applicant confirmed that he backed up "a bunch of stuff" on the afternoon that he submitted his two-week notice for leaving the company. Regarding his last download of information at Company A, Applicant testified as follows:

> [Department Counsel]: With regard to this last download, you didn't have permission to do that, is that right?
>
> [Applicant]: Not to take it, of course, no. But I did it every day anyways.[8]

When leaving Company A's employment, Applicant packed personal items in about 30 archive-type boxes. In his testimony, he indicated that he might have inadvertently placed the external hard drive in one of the boxes or just threw it in his briefcase. When he got home, he placed the boxes and other items from his office in his garage. He initially testified that he remembered seeing the external hard drive in his garage on either the night he left his job at Company A or the next day. When he saw the external hard drive, he thought "this is not mine, it's theirs." At some later point, he took all of the items, including the boxes, from his garage to Company B. In subsequent testimony and in his Answer to the SOR, he contradicted himself by saying he found the external hard drive at his new company. Specifically, he stated he realized he had the external hard drive "within a week or a month" of leaving Company A.[9]

Applicant also testified that he routinely used personal thumb drives to copy Company A data so that he could transfer it to other Company A work computers. He

[7] Applicant's Answer to the SOR.

[8] Tr. 44-48. Applicant stated that Company B did not bid against Company A on any competing work since he had been at Company B. *See* Applicant's Answer to the SOR.

[9] Tr. 46-54, 68; GE 2; Applicant's Answer to the SOR. Applicant first testified that he discovered the external hard drive in his garage the night he quit his job at Company A. *See* Tr. 50. Next, he testified that he discovered it in the garage the next day. *See* Tr. 53. Finally, he testified that he realized he had it in his new office "[w]ithin a week or a month" of leaving Company A. *See* Tr. 68.

testified that he copied data involving a Federal Government project from a Company A computer onto the personal thumb drive for use at Company B without authorization. Specifically, he testified:

> [Department Counsel]: All right, and so it's from that personal thumb drive that you had some [Company A] information and you uploaded that at [Company B]?
>
> [Applicant]: Yes, sir. It was just a drawing that we were working on that they (Company B) lost. This new company picked up, which they didn't do, but –
>
> [Department Counsel]: Did you have authority from [Company A] to both one, keep data, its data on that thumb drive, and then did you have [Company's A] permission to take that information off the thumb drive and give it to [Company B]?
>
> [Applicant]: No, sir.
>
> [Department Counsel]: So you didn't have any authority to do that either?
>
> [Applicant]; No, sir.
>
> [Department Counsel]: Why did you do that?
>
> [Applicant]: The thumb drive was just on my computer. The last thing I thought was I might need this one file for [the Federal Government project] because [Company A] was hiding all their files. They were denying the Government everything. They were hiding materials. They were stealing the data and that's why I think I took it. I just said I'm just going to take it so they can't lose this stuff. Because at that point, [Company A] had not uploaded those sites to the [name omitted] Government server which is what they did at the end of every project, so the Government had a legal copy.
>
> * * *
>
> [Department Counsel]: You didn't have authority from the Government or [Company A] to take the thumb drive to [Company B] and use that information at [Company B]?
>
> [Applicant]: No, sir. I did not.[10]

[10] Tr. 55-60, 62-65; GE 2. The unauthorized downloading of Company A information onto the personal thumb dive was not alleged in the SOR. Non-alleged misconduct may be considered to assess an applicant's credibility; to decide whether a particular adjudicative guideline is applicable; to evaluate

Applicant further testified that he notified the general manager of Company A about the wrongdoing of other Company A employees. However, he did not inform the general manager that he put the data involving the Federal Government project onto a personal thumb drive. He also indicated that he had no authority to backup Company A work onto his personal thumb drive.[11]

On November 4, 2011, which was ten days after Applicant left Company A's employment, a Joint Personnel Adjudication System entry was made that stated:

> On 10.25.11, [Applicant] obtained via: Unauthorized means company proprietary information, official Government Documentation, Cleared Facility Floor Plans and sensitive company financial data. Day of separation from company. FBI, DSS is currently investigating.[12]

In the OPM interview, Applicant indicated that he used a checklist when departing Company A and turned in all of Company A's property before he left except for the external hard drive because it was in one of his boxes. He also indicated that he told the human resources supervisor that he would return the external hard drive when he found it after going through the boxes.[13]

I did not find Applicant to be a credible witness. His testimony differed from his OPM interview. Applicant testified that, about a month after leaving Company A, he called the head of human resources at Company A to inform her that he had the external hard drive. He said that he had not called her earlier due to his procrastination. Two days after contacting her, an FBI agent and another federal investigator came to his house and questioned him about this matter for about two hours on his front porch. They did not search his house. He told them all the property in question was at Company B. The next day the FBI agent seized the external hard drive, personal thumb drive, and other items at Company B. At some later point, the FBI agent seized his Company B computer.[14]

---

evidence of extenuation, mitigation, or changed circumstances; to consider whether an applicant has demonstrated successful rehabilitation; or as part of the whole-person analysis. ISCR Case No. 03-20327 at 4 (App. Bd. Oct 26, 2006). The unauthorized downloading of information onto the personal thumb drive will be considered only for these limited purposes.

[11] Tr. 59, 72-75; AE A. In AE A, Applicant indicated that he informed a Government entity that Company A was copying a third company's data without authorization. He indicated that he believed Company A retaliated against him when they learned of this disclosure after he left Company A.

[12] GE 3.

[13] GE 2.

[14] Tr. 49, 52-56, 64-72, 79; GE 2.

Applicant also testified that, after leaving Company A, he ran into an employee of Company A at a department store. The employee informed Applicant that Company A was looking through the archive boxes that he left in the company's warehouse and asking if Applicant had been in that location. After talking to that employee, Applicant indicated that he "assumed" that Company A was conducting some type of inquiry concerning him, but he did not know exactly what was occurring. He also testified that he did not know whether he talked to the employee before or after he was contacted by the FBI and that his conversation with the Company A employee did not prompt him to contact the head of human resources to report he had the external hard drive. However, his statement that he did not know whether the conversation with the Company A employee occurred before or after he became aware of the FBI investigation does not make sense. If he had been aware of the FBI investigation before that conversation, he would have known why individuals were examining the archive boxes he placed in the warehouse and why they were asking questions about him. I find that Applicant's conversation with the Company A employee occurred before he became aware of the FBI investigation.[15]

In his Answer to the SOR, Applicant mentioned that a former employee of Company A stole a hard drive and erased company data without suffering any significant consequences. He believed that former employee still maintained a security clearance and was working as a federal employee.[16]

Applicant testified that he is not aware of any criminal charges being filed against him for this matter. The FBI returned the seized external hard drive to Applicant so that he could return it to Company A.[17]

Applicant presented letters of reference from a supervisor and coworkers that are highly complementary. The letters attested to his work ethic, dependability, trustworthiness, and integrity.[18]

## Policies

The President of the United States 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. *Department of the Navy v. Egan*, 484 U.S. 518, 527 (1988). The President has authorized the Secretary of Defense to grant 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*

[15] Tr. 68-75.

[16] Applicant's Answer to the SOR.

[17] Tr. 32-33, 61-62; GE 2; AE A.

[18] AE B-H.

*Classified Information within Industry* § 2 (Feb. 20, 1960), as amended. The U.S. Supreme Court has recognized the substantial discretion of the Executive Branch in regulating access to information pertaining to national security, emphasizing that "no one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988).

Eligibility for a security clearance is predicated upon the applicant meeting the criteria contained in the AGs. 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 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, to reach his decision.

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 of 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), Section 3. Thus, a clearance decision is merely an indication that the Applicant has or 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 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

### Guideline K, Handling Protected Information

AG ¶ 33 sets forth the security concerns for the handling of 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 unwillingness and ability to safeguard such information, and is a serious security concern.

I have considered all of the handling of protected information disqualifying conditions under AG ¶ 34 and the following are potentially applicable:

> (b) collecting or storing classified or protected information at home or in any other unauthorized location;
>
> (c) loading, drafting, editing, modifying, storing, transmitting, or otherwise handling classified reports, data, or other information on any unapproved equipment including but not limited to any typewriter, word processor, or computer hardware, software, drive, system, gameboard, handheld, "palm" or pocket device or other adjunct equipment; and
>
> (g) any failure to comply with rules for the protection of classified or other sensitive information.

Sufficient circumstantial evidence exists to establish that Applicant intentionally took the external hard drive from Company A without permission. He testified that he backed up "a bunch of stuff" to the external hard drive on the afternoon of the day he was leaving Company A, which is suspicious. He further indicated that he pre-packed his personal items before submitting his two-week notice, yet claimed the external hard drive was inadvertently placed in either a box or his briefcase. In the OPM interview, he indicated that he used a checklist when leaving and had turned in everything but the external hard drive because it was in one of the boxes. He stated that he told the human resources supervisor that he would return the external hard drive when he found it after going through the boxes. Conversely, he initially testified that he learned he had the external hard drive when he saw it in his garage the night he left Company A or the next day. He next testified that he realized that he had the external hard drive "within a week or a month" when it was at Company B. Even though he supposedly saw the external hard drive in his garage shortly after leaving Company A, he took it to Company B where it was eventually seized by the FBI. These and other inconsistencies cause me to give little weight to Applicant's testimony.

Applicant stated that he procrastinated in reporting to the head of human resources of Company A that he had found the external hard drive in his garage. He

made that report about a month after leaving Company A and two days before the FBI agent appeared at his house. He also testified that he ran into an employee of Company A and, based on their conversation, "assumed" an inquiry was being conducted that involved him. As noted above, I found that conversation occurred before he became aware of the FBI investigation. Sufficient circumstantial evidence exists to conclude that Applicant's conversation with the Company A employee is what prompted him to report to the head of human resources that he had the external hard drive.

Furthermore, Applicant's testimony regarding the personal thumb drive establishes that he had the intent to take property from Company A without its knowledge or authorization. His comments about the former employee who took Company A property without any significant consequences also tends to show that he may have believed the risk of consequences were slight if he took property. When the above pieces are put together, the picture becomes clear that Applicant intentionally took the external hard drive from Company A.

Applicant had no authority to take Company A proprietary data or official government information on the external hard drive and store that information at Company B. AG ¶ 34(b) applies. Applicant's loading of Company A proprietary information onto a Company A external hard drive when he was an employee of that company was authorized. AG ¶ 34(c) does not apply. No specific rule violations were established. AG ¶ 34(g) does not apply.

There are three handling of protected information mitigating conditions under AG ¶ 35. They are:

> (a) so much time has elapsed since the behavior, or it happened so infrequently or 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 individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities; and
>
> (c) the security violations were due to improper or inadequate training.

None of the mitigating conditions apply. Applicant's conduct is recent and casts doubt on his reliability, trustworthiness, and good judgment. No evidence of counseling or remedial security training was offered. Applicant knew that he should not have taken sensitive data from Company A to Company B, but he intentionally did so.

**Guideline M, Use of Information Technology Systems**

AG ¶ 39 expresses the security concern pertaining 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 reliably 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, firmware, and data used for the communication, transmission, processing, manipulation, storage, or protection of information.

AG ¶ 40 describes conditions that could raise a security concern and may be disqualifying. The following are potentially applicable:

> (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.

The discussion of the facts under Guideline K applies equally here and is incorporated under this guideline. Applicant removed the external hard drive from Company A without its authorization. He knew taking such property for use at Company B was prohibited. AG ¶ 40(f) applies.

There are three use of information technology systems mitigating conditions under AG ¶ 41. They are:

> (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 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
>
> (c) the conduct was unintentional or inadvertent and was followed by a prompt, good-faith effort to correct the situation and by notification of supervisor.

For the reasons discussed under Guideline K, none of the Guideline M mitigating conditions apply in this case.

## 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(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.

Under AG ¶ 2(c), 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.

I considered the potentially disqualifying and mitigating conditions in light of all relevant facts and circumstances surrounding this case. I have incorporated my comments under Guidelines K and M in my whole-person analysis. Some of the factors in AG ¶ 2(a) were addressed under those guidelines, but some warrant additional comment.

Applicant has worked for a defense contractor and has held a security clearance for many years without incident. He is a valued employee. Nevertheless, security concerns remain in this case. Applicant admitted that he downloaded data from a Company A computer onto a personal thumb drive without its authorization. He also intentionally took Company A's external hard drive when he was leaving that company's employment. Such actions were a breach of trust.

Overall, the record evidence leaves me with questions and doubts about Applicant's suitability for a security clearance. Therefore, I conclude Applicant has not mitigated the security concerns arising under Guidelines K and M.

## 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 K: | AGAINST APPLICANT |
| Subparagraph 1.a: | Against Applicant |

| | |
|---|---|
| Paragraph 2, Guideline M: | AGAINST APPLICANT |
| Subparagraph 2.a: | Against Applicant |

## Decision

In light of all the circumstances presented by the record, it is not clearly consistent with the national interest to grant or continue Applicant's eligibility for a security clearance. Eligibility for access to classified information is denied.

_____
James F. Duffy
Administrative Judge