DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 12-07997
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Caroline H. Jeffreys, Esq., Department Counsel
For Applicant: *Pro se*

07/10/2013

Decision

COACHER, Robert E., Administrative Judge:

Applicant mitigated the security concerns under Guideline M, use of information technology systems, and Guideline E, personal conduct. Applicant's eligibility for a security clearance is granted.

Statement of the Case

On February 8, 2013, the Department of Defense Office (DOD) issued Applicant a Statement of Reasons (SOR) detailing security concerns under Guideline M, use of information technology systems, and Guideline E, personal conduct. DOD acted under Executive Order 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the adjudicative guidelines (AG), effective within the Department of Defense on September 1, 2006.

Applicant answered the SOR on March 2, 2013. He requested a hearing before an administrative judge. The case was assigned to me on April 24, 2013. The Defense Office of Hearings and Appeals (DOHA) issued a notice of hearing on May 10, 2013, with a hearing date of May 29, 2013. The hearing was convened as scheduled. The Government offered exhibits (GE) 1 through 4, which were admitted into evidence without objection. Applicant testified, presented one witness, and offered exhibits (AE) A through K that were admitted into evidence without objection. DOHA received the hearing transcript (Tr.) on June 6, 2013.

Findings of Fact

In Applicant's answer to the SOR, he admitted the allegation listed in ¶ 1.a, but denied the allegations listed in ¶¶ 2.a and 2.b. After a thorough and careful review of the pleadings, testimony, and exhibits, I make the following findings of fact.

Applicant is 43 years old. He has been married for 17 years. He has two children. He holds a master's degree in aerospace engineering. He currently works for a defense contractor as an engineer. He began working for his current employer in November 2011, where he supervises over 200 people. From March 2005 until August 2011, he worked for a different defense contractor as the director of engineering. He was also the facility security officer (FSO). He resigned from that position after a dispute arose with the company owner about his future employment with the company. He has not had a security-related incident since he has held a security clearance in 2002.[1]

Applicant's conduct raised in the SOR includes: (1) using his company's network to copy company information, including sensitive data, onto a personal computer hard drive (SOR ¶¶ 1.a, 2.b); (2) as a result of copying the company data, he was terminated from employment. (SOR ¶ 2.a).

In 2005, Applicant was working for a defense contractor when he was approached by Mr. B, who was starting his own company, with an offer of employment. Applicant was excited about getting in on the ground level of this new company, which at the time, had about five employees and sales of about $300,000 per year. In March 2005, he joined the company. He also became a minority shareholder in the company (10% interest) and he and Mr. B formed a partnership to purchase the company's building. Soon, the company flourished and sales increased to about $10,000,000 per year. Applicant believed his efforts were a significant factor in the company's growth.[2]

After coming back from a vacation and returning to work in August 2011, Applicant noticed that his relationship with Mr. B was strained. Mr. B was not speaking to him. On August 10, 2011, Applicant was called into Mr. B's office and was accused of becoming a poor performer and insubordinate. Mr. B then told Applicant to choose his

[1] Tr. at 6, 35; GE 1, 4.

[2] GE 4; AE I.

termination date. Applicant asked for two days to think about it. He was at a loss as to why Mr. B was acting this way. Applicant was called that evening by a coworker who suggested that Applicant should request an alternate working arrangement (such as working from home) so that he could stay with the company. On August 11, 2011, Applicant again met with Mr. B. Applicant suggested an alternate work arrangement and Mr. B indicated that he wanted to consider the proposal and would respond on the following Monday. In anticipation that his request for an alternate work site would be approved, and to ensure he could support his customers, on August 12, 2011, he copied unclassified files from the company's network onto an external hard drive. This would allow him access to necessary files when he worked from home. On Monday, August 15th at 9:00 am, Applicant met with Mr. B and they agreed that Applicant would remain an employee until October 31, 2011, at which time the company would assess whether he would continue beyond then as a consultant. During this time, he would work off site. The terms of this arrangement were denoted in an unsigned written document. The record does not reflect who authored the document. Also on August 15th, sometime after 9:00 am and before 11:00 am, Applicant was told to report to Mr. B's office. Mr. B asked him whether he had copied company materials onto an external drive (Mr. B knew this had happened because the company's computer staff was monitoring Applicant's computer activites). Applicant admitted that he copied the files so that he would be able to work from home. He explained that he only copied technical data and not proprietary information. Mr. B accused Applicant of theft and threatened legal action if he did not sign an affidavit stating he did not keep any of the copied information. Mr. B demanded the copied information be returned. Later that same day, Applicant returned the hard drive containing the copied information. He also sent Mr. B an email explaining what was on the drive. In the email, he also offered his apology for copying the files. He stated he did so with no malicious intent, but only with a thought to help the company. The next day Applicant submitted a resignation letter to Mr. B.[3]

Applicant copied the documents using his own account and he did not attempt to hide his act of accessing the account. He did not attempt to disclose the information outside of proper channels. The documents that were accessed were documents that he used in the regular course of business and that he had authority to access on a regular basis. He did not believe he violated any company policies or procedures when he copied the documents. His apology email reflected his belief that he disappointed Mr. B rather than that he violated security procedures. He had no motive to harm the company since he remained a 10% owner. No evidence was offered to show that any specific company policy or procedure was violated when Applicant copied the documents.[4]

Applicant was successful in his unemployment claim against his former company. After receiving evidence from both Applicant and the company, a determination was made that Applicant's departure was involuntary because of

[3] Tr. at 39-40; GE 3, 4; AE A, B, F.

[4] Tr. at 40-41, 60, 64, 68, 74, 75-76; GE 3, 4; AE A, B.

unreasonable criticisms made by his employer. His claim for unemployment was approved in October 2011.[5]

The company did not conduct an administrative inquiry into the events concerning Applicant's copying of the files and his resulting resignation until December 22, 2011. An entry into the DOD database for security incidents did not occur until January 3, 2012. Applicant pointed out that the administrative inquiry was submitted after he and Mr. B negotiated a buyout of Applicant's interest in the building ownership partnership.[6]

Applicant called one witness, the facilities security officer for his current employer, who testified that she has daily contact with him and has never experienced any security related issues concerning him. She also has no security concern about him, nor has she heard of such concerns by others. She recommended that his clearance be reinstated.[7]

Applicant presented the statements of several coworkers and former coworkers, including his current employer's president and vice-president. All the statements recommend him for a security clearance. He is characterized as loyal, trustworthy, and a man of integrity.[8]

Policies

When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the adjudicative guidelines. In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially disqualifying conditions and mitigating conditions, which are used 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, these guidelines are applied in conjunction with the factors listed in the adjudicative process. The administrative judge's overarching adjudicative goal is a fair, impartial, and commonsense decision. According to AG ¶ 2(c), 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.

[5] Tr. at 38, 46; AE B.

[6] Tr. at 53-54; AE H-K.

[7] Tr. at 87-93.

[8] AE E.

The protection of the national security is the paramount consideration. AG ¶ 2(b) requires that "[a]ny doubt concerning personnel being considered for access to classified information will be resolved in favor of 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.

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 applicant or proven by Department Counsel, and has the ultimate burden of persuasion to obtain a favorable security 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 that an applicant may deliberately or inadvertently fail to 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 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 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. I have considered the following as potentially relevant:

(a) illegal or unauthorized entry into any information technology system or component thereof;

(c) use of any information technology to gain unauthorized access to another system or to a compartmented area within the same system;

(e) unauthorized use of a government or other information technology system; and

(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.

Although Applicant was not given explicit permission to copy the files on this occasion, he had done so before, with the apparent authority to do so, in order to conduct work away from the office. However, what complicated this event was that Applicant and his employer were in the midst of changing Applicant's work duties and responsibilities, thereby calling into question whether he had the authority to copy the files this time. I find that Applicant acted in good faith when he copied the unclassified files and the Government failed to produce evidence showing that he violated any specific company policy by copying the files. I find none of the above disqualifying conditions apply.

I also have considered all of the mitigating conditions under AG ¶ 41 and in the event my conclusions on the non-applicability of the above disqualifying conditions are overturned, I 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.

Applicant's actions in copying the files occurred in August 2011. He no longer works for the company in question. He supervises over 200 employees and, other than those alleged in the SOR, has never had a security-related incident. Both previous coworkers and present coworkers attest to his reliability, trustworthiness, and good judgment. Given the circumstances that were ongoing when he copied the files, I find that such a situation is unlikely to recur. AG ¶ 41(a) applies.

Guideline E, Personal Conduct

AG ¶ 15 expresses the security concern for 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.

AG ¶ 16 describes conditions that could raise a security concern and may be disqualifying in this case. The following disqualifying condition is potentially applicable:

> (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 person may not properly safeguard protected 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 other government protected information:
>
> (2) disruptive, violent, or other inappropriate behavior in the workplace;
>
> (3) a pattern of dishonesty or rule violations; and,
>
> (4) evidence of significant misuse of Government or other employer's time or resources.

Although Applicant officially resigned from his position, there is little doubt that his copying of the files would have led to termination had he not resigned. However, this termination would not be as a result of Applicant misusing information technology or because of rules violations, but because of Mr. B's subjective decision to terminate him. Additionally, the above analysis that he did not misuse the company's information technology systems also applies to SOR ¶ 2.b under the personal conduct disqualifying. AG ¶ 16(d) does not apply.

The guideline also includes conditions that could mitigate security concerns arising from personal conduct. In the event my conclusion on the non-applicability of the above disqualifying condition is overturned, I have considered all of the mitigating conditions under AG ¶ 17 and found the following relevant:

> (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.

Applicant's actions in copying the files occurred in August 2011. He no longer works for the company in question. He supervises over 200 employees and, other than those alleged in the SOR, has never had a security-related incident. Both previous coworkers and present coworkers attest to his reliability, trustworthiness, and good judgment. Given the circumstances that were ongoing when he copied the files, I find that such a situation is unlikely to recur. AG ¶ 17(c) applies.

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.

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 the facts and circumstances surrounding this case. I considered Applicant's service to his company before the events that led to his resignation. I also considered the circumstances that resulted in his resignation. Additionally, I considered the strong recommendations he received from coworkers concerning his honesty, reliability, and trustworthiness. I also considered that this incident occurred almost two years ago, with a different company, and that he has had no security incidents with his new employer. Applicant met his burden to provide sufficient evidence to mitigate the security concerns.

Overall, the record evidence leaves me with no questions or doubts about Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude Applicant mitigated the security concerns arising under Guideline M, use of information technology systems, and Guideline E, personal conduct.

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 E:	FOR APPLICANT
Subparagraphs 2.a-2b:	For Applicant

Conclusion

In light of all of 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 access to classified information is granted.

_____
Robert E. Coacher
Administrative Judge