DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 14-04603
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Daniel F. Crowley, Esq., Department Counsel
For: Applicant: John W. McKendree

01/27/2016

_____

Decision

_____

COACHER, Robert E., Administrative Judge:

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

Statement of the Case

On February 17, 2015, the Department of Defense (DOD) issued Applicant a Statement of Reasons (SOR) detailing security concerns under Guideline K, Guideline M, and Guideline E. The DOD acted under Executive Order 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), effective within the DOD after September 1, 2006.

Applicant answered (Ans.) the SOR on March 3, 2015, and requested a hearing before an administrative judge. The case was assigned to me on July 1, 2016. The Defense Office of Hearings and Appeals (DOHA) issued a notice of hearing on July 2, 2015, with a hearing date of July 30, 2015. The hearing was held as scheduled. The Government offered the testimony of one witness and exhibits (GE) 1 through 4, which were admitted into the record without objection. Hearing Exhibits (HE) included Department Counsel's discovery letter (HE I), the Government's exhibit list (HE II), and relevant portions of the National Industrial Security Program Operating Manual (NISPOM) (HE III).[1] Applicant testified, presented two witnesses, and produced exhibits (AE) 1 and 2 that were admitted into the record without any objection. DOHA received the hearing transcript (Tr.) on August 7, 2015.

Findings of Fact

In Applicant's answer to the SOR, he admitted the allegation listed at ¶ 1.a, with explanations, and denied the remaining allegations. After a thorough and careful review of the pleadings, testimony, and exhibits, I make the following additional findings of fact.

Applicant is 50 years old. He is married and has one child. He has worked for his current defense contractor since 2013. He is a systems administrator. He has held a secret clearance since 2005. He has a bachelor's degree.[2]

The allegations against Applicant include failing to properly secure a locking device in March 2014 and committing information security violations that led to his termination of employment from a previous government contractor. Those violations were cross-alleged under Guidelines K, M, and E.

In March 2014, while working for his current employer, Applicant was responsible for securing a locking device. Because of vision problems caused by two eye surgeries, his peripheral vision was affected, and he did not see a lanyard indicating that the safe was open. The security infraction was discovered, an investigation ensued, but it was determined no security compromise occurred. He was issued a verbal security warning and was given security refresher training. He also requested to be relieved of his duties to secure the device, and his request was granted. He has had no further security incidents.[3]

Applicant was hired by his former employer as a contract administrator in November 2012. His supervisor was located in another city. Upon assuming his position, he did not receive security training. He believed this occurred because he was hired as a level 4 administrator and it was assumed by the company he should know

[1] I took administrative notice of relevant NISPOM language. *See* Tr. at 17.

[2] GE 1.

[3] Tr. at 121-122; Ans., GE 4; AE 2.

about systems administration security. The Government did not produce his training record at the company. A witness for the Government made reference to a training document that all employees must sign, but that document was not produced. Applicant was not given training or direction concerning how to perform his duties. He was told by his off-site supervisor to follow the examples of the other team members.[4]

In July to August 2013, Applicant was investigated by the company's information systems security manager (ISSM) for failure to follow proper information security procedures. The inquiry found that: (1) Between November 2012 and July 2013, Applicant created multiple user accounts without security permission or documentation; (2) Between January and July 2013, Applicant logged onto the network system directly as "root" and failed to document such in a root login log; (3) In May 2013, Applicant changed the security posture of his workstation without notifying security or receiving approval; (4) Applicant copied the contents of a folder from a server without proper permission; and (5) The ISSM felt Applicant was not forthright about his actions during his inquiry. Applicant's response to these findings was as follows: (1) He created additional user accounts to use as practice accounts to figure out potential problems. He also created accounts to develop a new directory access protocol. He was not told by anyone he needed to seek permission to create these additional accounts. (2) He logged in as a root user because his normal account stopped working and to convert a directory. He was never told about using a login log to note when he used root access. He did not see a login log at the workplace or anyone using such a log. (3) He changed the security posture of his workstation to allow him to make directory changes, which he believed was part of his job. He was not given any instruction on how to perform this task. (4) He had no training on the server type on which he was working and thought he was doing what he was supposed to do. (5) I found Applicant's testimony credible. He did not provide false or misleading information to the investigator.[5]

Applicant's two witnesses testified that they have worked with him since he began working for his current employer and both expressed their beliefs that he complies with all security procedures and is a trustworthy concerning security procedure. Similar sentiments were expressed by a former supervisor who worked with Applicant previously.[6]

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

[4] Tr. at 31, 47, 68, 71-76; Ans., GE 4.

[5] Tr. at 75-90, 96; GE 2, 4.

[6] Tr. at 128-138; AE 1.

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.

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 K, Handling Protected Information

AG ¶ 33 expresses the security concern pertaining 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.

I have considered all the handling protected information disqualifying conditions under AG ¶ 34 and determined the following apply:

> (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.

Applicant failed to comply with proper procedure when he did not secure a locking device for which he was responsible. The creation of multiple user accounts, logging in as a root user and not recording that login in a log, changing the security posture of his workstation, and copying a folder from a server were not in accordance with the company's proper procedures. Both AG ¶¶ 34(c) and (g) apply.

All the mitigating conditions for handling protected information under AG ¶ 35 were considered and the following were found relevant under these circumstances:

> (a) so much time has elapsed since the behavior, or it has happened so infrequently or under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or good judgment;
>
> (b) the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities; and
>
> (c) the security violations were due to improper or inadequate training.

Applicant's actions can be considered remote since they occurred in September in 2013 and 2014. He has not experienced another security issue since that time. On the contrary, he has been recognized by his peers as having acute security awareness. He provided persuasive evidence to show that sufficient time has passed since the incidents, that any security issues are unlikely to recur, and that his current reliability, trustworthiness, and good judgment are not in doubt. AG ¶¶ 35(a) and 35(b) apply.

Applicant made a credible case that he was not properly trained in the security procedures that he was expected to utilize in his former position. The Government's evidence failed to refute the lack of training. AG ¶ 35(c) applies.

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;
>
> (b) illegal or unauthorized modification, destruction, manipulation or denial of access to information, software, firmware, or hardware in an information technology system; and
>
> (e) unauthorized use of a government or other information technology system.

The analysis above for the Guideline K allegations also applies under Guideline M. AG ¶¶ 40(a), 40(b), and 40(e) apply.

I also have considered all of the mitigating conditions under AG ¶ 41 and 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 can be considered remote since they occurred in September in 2013. He has not experienced another security issue concerning information systems security since that time. On the contrary, he has been recognized by his peers as having acute security awareness. He provided persuasive evidence to show that

sufficient time has passed since the incidents, that any security issues are unlikely to recur, and that his current reliability, trustworthiness, and good judgment are not in doubt. 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:

> (b) deliberately providing false or misleading information concerning relevant facts to an employer.

Although no falsification is specifically alleged in SOR, by implication it was raised by the evidence (GE 2) and is addressed here.[7] The evidence does not support the allegation that Applicant was not truthful when he was interviewed by the company's investigator. Applicant refuted the personal conduct guideline allegation. AG ¶ 16(b) does not apply.

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.

[7] AG ¶¶ 16(c) and 16(d) do not apply because the underlying conduct is addressed under Guidelines K and M.

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 that Applicant's last security incident occurred in 2014 without recurrence. I considered the lack of training that he received, and his physical handicap that led to the security concerns. I also considered that he has been recognized for by his peers as being security conscious. All of which demonstrate his permanent behavior changes toward security issues and the unlikeliest chance of recurrence. Applicant met his burden and provided sufficient evidence to mitigate the security concerns.

Overall the record evidence leaves me without 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 K and Guideline M. I also find that Applicant refuted the Guideline E security concern.

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 K:	FOR APPLICANT
Subparagraphs 1.a-1.b:	For Applicant
Paragraph 2, Guideline M:	FOR APPLICANT
Subparagraph 2.a:	For Applicant
Paragraph 3, Guideline E:	FOR APPLICANT
Subparagraph 3.a:	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 eligibility for a security clearance. Eligibility for access to classified information is granted.

_____
Robert E. Coacher
Administrative Judge