DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 14-04881
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Adrienne M. Strzelczyk, Esq., Department Counsel
For: Applicant: *Pro se*

02/29/2016

_____

Decision

_____

COACHER, Robert E., Administrative Judge:

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

Statement of the Case

On March 16, 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 April 1, 2015, and requested a hearing before an administrative judge. The case was assigned to me on October 1, 2015. The Defense Office of Hearings and Appeals (DOHA) issued a notice of hearing on October 5, 2015, with a hearing date of October 20, 2015. The hearing was held as scheduled. The Government offered exhibits (GE) 1 through 3, which were admitted into the record without objection. Applicant and one witness testified. Applicant offered no documents at the hearing, but the record was kept open and he offered exhibit (AE) A in a timely post-hearing submission, which was admitted with no objection. DOHA received the hearing transcript (Tr.) on October 30, 2015.

Findings of Fact

In Applicant's Ans., he admitted all the allegations, with explanations. After a thorough and careful review of the pleadings, testimony, and exhibits, I make the following additional findings of fact.

Applicant is 35 years old. He is married and has one child. He has worked for his current employer, a defense contractor, since 2010. He is a systems administrator. He has held a secret clearance since 2004. He has a master's degree.[1]

The allegations against Applicant include failing to comply with closed area procedure by placing a file directory of a higher classification on a lower level disk drive in January 2013, resulting in a security infraction; improperly downloading material while completing a work task in a lab environment in March 2013, resulting in a security violation; and failing to comply with closed area procedures by disclosing unclassified program information that required enhanced protection procedures by using an unsecured telephone in March 2013, resulting in a security infraction. These incidents were cross-alleged under Guidelines K, M, and E.

In January 2013, Applicant was tasked to perform duties that he had not done before. He was responsible for visually verifying thousands of lines of script and missed a classified item that should not have been there. That same classified item was also missed by a security engineering team as well. There was no compromise, since the people who noticed the classified script were cleared personnel. Applicant was given a verbal counseling by his supervisor for this incident (SOR ¶ 1.a). Applicant acknowledged his mistake and talked to his supervisor about how to accomplish the task correctly. He was removed from this tasking and has not performed it since the incident. Additionally, the verification process has been changed and improved because of the incident.[2]

In March 2013, Applicant was performing another duty, which was part of the same tasking that resulted in his January 2013 infraction. In this subtask, he was to

[1] Tr. at 5, 21-22, 31; GE 1.

[2] Tr. at 22-24, 26, 28, 38-39; Ans., GE 3.

transfer media from a backup storage drive to a boot drive using new equipment that was not covered by existing procedures. Procedures existed for how such a transfer was to take place using different equipment. However, new procedures were being written, but were not completed at this time. Because the transfer that Applicant was tasked to complete was time sensitive, he was directed to proceed even though the new transfer procedures were not finalized. The old procedures failed to address the type of transfer he was about to complete. With this ambiguity, he now realizes he should have stopped the transfer and sought guidance from his security team. He was cited for a security violation (SOR ¶ 1.b). After the transfer, the lab discs were examined and no compromise took place. Applicant talked to senior members of the team about how to accomplish future transfers properly. He accepted responsibility for his actions and has learned from this mistake. He no longer performs this task.[3]

Later in March 2013, when the incident stated in SOR ¶ 1.b was under investigation by the company's security division, Applicant was contacted by telephone by a security representative and asked questions about the incident. During the call, Applicant revealed some unclassified program information that required enhanced protection procedures and which was not to be revealed over an open telephone line. Applicant admitted his mistake in disclosing this information. He explained that he was nervous and upset about the investigation. His disclosure was inadvertent and he immediately got off the phone and went to the security office to finish the conversation. He received a verbal warning for this incident (SOR ¶ 1.c). He has taken corrective measures to insure that he will not disclose sensitive information over the telephone. He has not had another security incident since March 2013.[4]

Applicant's immediate supervisor testified that he was fully aware of the three security incidents that form the SOR. He has supervised Applicant since 2010. He described Applicant as a hard working model employee with great integrity. He believes Applicant's actions were inadvertent. He can see how the incidents could have happened to anyone in Applicant's position. He provided an example by stating that the person who succeeded Applicant with the tasks also made similar mistakes. He was upset when he heard the circumstance concerning the SOR ¶ 1.c allegation (telephone disclosure) because he believed that the security division should not have put Applicant in the position of discussing the investigation over the telephone in the first place. He believes they were wrong to do so. He continues to support Applicant for a security clearance. He believes Applicant made honest mistakes and has learned from them.[5]

[3] Tr. at 25; Ans., GE 3.

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

[5] Tr. at 53-64.

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.

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:

> (a) deliberate or negligent disclosure of classified or other protected information to unauthorized persons, including but not limited to personal or business contacts, to the media, or to persons present at seminars, meetings, or conferences;
>
> (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;
>
> (g) any failure to comply with rules for the protection of classified or other sensitive information; and
>
> (h) negligence or lax security habits that persist despite counseling by management.

Applicant failed to comply with proper procedures as outlined in the SOR allegations. AG ¶¶ 34(a), 34(c), and 34(g) apply, but because there was no evidence of counseling by management before the incidents, AG ¶ 34(h) does not 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 January and March 2013 and resulted from the same general tasking to him. He has not experienced another security issue since that time. On the contrary, he has been recognized by his supervisor as acknowledging his mistakes and learning from them. 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 there was ambiguity concerning his responsibilities to properly perform the tasks which resulted in the SOR ¶¶ 1.a and 1.b allegations. 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:

(d) downloading, storing, or transmitting classified information on or to any unauthorized software, hardware, or information technology system; and

(g) negligence or lax security habits in handling information technology that persist despite counseling by management.

The analysis above for the Guideline K allegations also applies under Guideline M. AG ¶ 40(d) applies, but because there was no evidence of counseling by management before the incidents, AG ¶ 40(g) does not 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 between January and March 2013 and were all related to the same tasking. He has not experienced another security issue concerning information systems security since that time. On the contrary, his supervisor vouched for his trustworthiness and expressed his satisfaction that Applicant learned from this incident and will not let it happen again. 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:

> (c) credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any other single guideline, but which, when considered as a whole, supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the person may not properly safeguard protected information.

Between January and March 2013, Applicant failed to comply with proper procedure, which resulted in three security incidents. AG ¶ 16(c) applies.

AG ¶ 17 describes conditions that could raise a security concern and may be disqualifying. I have considered the following as 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; and
>
> (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.

Applicant sought advice from management on how to deal with similar situations in the future and is dedicated to not making the same mistakes again. Other people have made similar mistake and as a result security procedures have been changed. His own security people set him up for failure by asking him questions concerning the investigation over the telephone. His direct supervisor is convinced that Applicant learned from this experience and vouches for his trustworthiness, good judgment, and reliability. Similar incidents are unlikely to recur. AG ¶¶ 17 (c) and 17(d) 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.

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 2013 without recurrence. I considered the lack of training that he received, the mission requirements he was subject to, and the confusion over the proper procedures to follow. I also considered that he admitted his mistakes and showed initiative in seeking improvement. 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, Guideline M, and Guideline E.

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.c:	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