DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 11-09219
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Jeff Nagel, Esquire, Department Counsel
For Applicant: *Pro se*

May 7, 2014

Decision on Remand

CEFOLA, Richard A., Administrative Judge:

Applicant submitted her Electronic Questionnaires for Investigations Processing (e-QIP) on December 17, 2010. On August 7, 2013, the Department of Defense (DOD) issued a Statement of Reasons (SOR) detailing the security concerns under Guideline K for Applicant. The action was taken 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 after September 1, 2006.

Applicant acknowledged receipt of the SOR on August 15, 2013. She answered the SOR in writing on August 31, 2013, and requested a hearing before an Administrative Judge. DOHA received the request soon thereafter, and I received the case assignment on September 23, 2013. DOHA issued a notice of hearing on September 24, 2013, and I convened the hearing as scheduled on October 24, 2013. The Government offered Exhibits (GXs) 1 through 8, which were received without objection. Applicant testified on her own behalf, and called her first line supervisor to

testify on her behalf. DOHA received the transcript of the hearing (TR) on November 4, 2013. I granted Applicant's request to keep the record open until November 22, 2013, to submit additional matters. On November 15, 2013, she submitted Exhibit (AppX) A, which was received without objection. As the undersigned was on sick leave, Friday November 22, the record closed on Monday, November 25, 2013. Based upon a review of the pleadings, exhibits, and testimony, eligibility for access to classified information was granted.

Department Counsel appealed this Decision. On March 31, 2014, the Appeal Board remanded the Decision. The Appeal Board avers, in part, the following: "Once it is established that an applicant has committed security violations, he or she has a 'very heavy burden' to surmount in mitigating the concerns arising therefrom, insofar as security violations 'strike at the heart of the Industrial Security Program.'"

The Appeal Board continues:

> In this case, the Judge's analysis failed to address significant record evidence, such as the number of infractions committed by Applicant and that these infractions occurred despite prior training. . . . Moreover, the record demonstrates that Applicant's subsequent offenses [two through five] occurred against a background of repeated verbal and written corrective action. The extent to which Applicant had been placed on notice of the security requirements of her job, and to which she received adverse action regarding her infractions, are relevant in evaluating the seriousness of her conduct. This evidence is crucial to an adequate mitigation analysis, bearing as it does on the foreseeability of future misconduct that strikes at the heart of the security clearance process. The Judge's analysis makes no reference to this evidence, nor does it examine the evidence as a whole in light of Applicant's "heavy burden" of persuasion.

Findings of Fact

In her Answer to the SOR, Applicant admitted the factual allegations in the Subparagraphs of the SOR, with explanations.

Guideline K - Handling Protected Information

Applicant served honorably on active duty with the U.S. Army (Employer 1) from November of 1984 to May of 1987. (TR at page 36 line 12 to page 38 line 14, and AppX A the last page.) She held a security clearance while on active duty, and had no security clearance violations. (*Id*.) She "was a Counter-Signals Intelligence Specialist"; and as such, it can be assumed she had "security training." (TR at page 37 lines 2~14.) After leaving active duty, Applicant went to college. (Tr at page 40 line 9 to page 41 line 24.) In 2001, while still attending college, she began working for Employer 2, in a job

that required a security clearance. It can also be assumed she again had "security training." She had no security clearance violations while working for Employer 2. (*Id*.)

In 2004, Applicant began working for Employer 3, in a job that also required a security clearance. She has admitted to five security violations, as delineated below in Subparagraphs 1.a.~1.e., from April of 2008 to July of 2010, while working for Employer 3. In 2004, she received an "initial indoctrination briefing," and thereafter "has completed annual security refresher training," according to Employer 3. (GX 7 at page 6.)

1.a. and 1.b. The first two incidents occurred in April and again in June of 2008. Applicant was required to spin the tumbler on the door when departing the "secured environment" she worked in. (TR at page 43 line 7 to page 50 line 21, and GXs 4 and 5.) She describes the first incident in the following terms: "Well, as I was leaving . . . I believe I dropped my keys. I had shut the door, dropped my keys and purse and stood back up, thought I had spun the dial already and signed out." (TR at page 45 lines 11~15.) She did not spin the dial; and as a result, "the room was not properly secured." (GX 4 at page 4.) Applicant received a verbal warning as a result of this incident. (*Id*.)

She describes the second incident in the following terms: "so, I shut the door and proceeded to sign out and spin the dial but forgot that I left something inside. So, I . . . did the code to get back in. Went in and got my keys or purse or whatever it was; came back out and I don't know what I was thinking - - just signed out." (TR at page 48 lines 19~25.) She again forgot to spin the dial; and as a result, "the room was not properly secured." (GX 5 at page 8.) Applicant received a verbal and a written warning as a result of this incident.

1.c. In March of 2009, the third incident occurred. (GX 6.) Applicant "grabbed" what she thought was an unclassified file, and "burned" it to a "CD." (TR at page 52 lines 10~24.) She took the CD and put it into "an unclassified network." (TR at page 53 lines 9~24.) Applicant then describes what happened:

> As I was copying a folder over into the [unclassified] computer, and I am watching the file names go over, I saw a name of a file that was not supposed to be there and . . . I disconnected the network, stopped the process, shut the computer down. I got up from my desk, went to security and notified Security what had happened." (*Id*.)

Applicant received a memorandum of concern as a result of this self-reported incident.

1.d. In March of 2010, the fourth incident occurred. (GX 7.) Applicant failed to properly secure a classified tape. (TR at page 57 line 17 to page 63 line 13.) She describes the fourth incident in the following terms: "I was leaving the program. . . . I had signed for the safe. . . . I didn't have Security come in and inventory the safe when I left." (TR at page 59 lines 11~16.) "So, my leaving, left the safe in my name when they

finally went in after I had gone and found the tape missing, it was my fault." (TR at page 60 line 24 to page 61 line 2.) The missing tape was eventually accounted for. (TR at page lines 12~13.) Applicant was provided security training as a result of this incident.

1.e. In July of 2010, the last incident occurred. (GX 8.) Applicant wrongfully uploaded classified data onto an unclassified network. (TR at page 63 line 15 to page 68 line 6.) She describes the fifth incident in the following terms:

> . . . we put this document on an unclassified network . . . Well I left the program. New people came in and were going through the documentation that we had previously done, found . . . they say [the document] should have been classified. Unfortunately, just because you don't know doesn't mean it's okay. (TR at page 66 line 14 to page 67 line 3.)

Applicant was issued a security violation as a result of this incident.

Since coming to work for Employer 4 in 2010, Applicant has had no security clearance violations, and her first-line supervisor attests that she is most trustworthy. (TR at page 17 line 23 to page 32 line 22, and AppX A at page 1; *see also* AppX A at pages 2~9.) Her supervisor, who testified on Applicant's behalf, also avers, in part, the following in a written statement:

> Professionally, I have been able to observe her for the last 3 years and believe there is no risk to the US Government in continuing with her current DoD security clearance as well as the higher level's (sic) where she operates. In fact, her unblemished history of working within my program where she's been exhibiting high standards will prove that whatever hiccups happened prior to her on-boarding with . . . [her current program] will show those infractions help (sic) mold her to the OPSEC [Operations Security] superstar she is for the program. (AppX A at page 1.)

Policies

When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the adjudicative guidelines (AG). In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially disqualifying conditions and mitigating conditions, which are useful 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. (AG Paragraph 2.) The administrative judge's over-arching adjudicative goal is a fair, impartial and commonsense decision. According to AG Paragraph 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 Paragraph 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. Likewise, I have avoided drawing inferences grounded on mere speculation or conjecture.

Under Directive Paragraph E3.1.14, the Government must present evidence to establish controverted facts alleged in the SOR. Under Directive Paragraph E3.1.15, the applicant is responsible for presenting "witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by applicant or proven by Department Counsel. . . ." The applicant has the ultimate burden of persuasion as to obtaining 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 the Applicant may deliberately or inadvertently fail to protect or 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

The security concern relating to the guideline for Handling Protected Information is set out in AG Paragraph 33:

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

The guideline notes several conditions that could raise security concerns. Under Subparagraph 34(c), "*loading . . . classified reports, data, or other information on any*

unapproved equipment" is potentially disqualifying. Similarly under Subparagraph 34(g), *"any failure to comply with rules for the protection of classified or other sensitive information*" may raise security concerns. Finally, under Subparagraph 34(h) "*negligence or lax security habits that persist despite counseling by management*." Applicant had five security violations prior to July of 2010, while working for Employer 3, and she received security training prior to and after these incidents. However, I find a countervailing Mitigating Condition that is applicable here. Under Subparagraph 35 (a), when "*so much time has elapsed since the behavior . . . that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or good judgment, . . .*" such facts may be mitigating. Applicant's actions were, for the most part, due to negligence. Applicant's admitted violations, while employed by Employer 3, are not symptomatic of who she is today. The last incident occurred close to four years ago in July of 2010. Her current supervisor testified at length as to her "unblemished history." (TR at page 17 line 23 to page 32 line 22.)

Applicant also testified credibly that she has learned from her past mistakes. She avowed, in part, the following: "Since I have been on another program that has its two-fold . . . higher classifications, I have been so diligent and so cognizant of what I handle, what I'm doing for my customer, for the Government. This scared me so bad that I think I am hyper-vigilant now." (TR at page 71 lines 3~9). I find that she is a most reliable and trustworthy employee for her current employer, as attested to by her supervisor.

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 Applicant's conduct and all the circumstances. Under Paragraph 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.

The administrative judge should also consider the nine adjudicative process factors listed at AG Paragraph 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.

I considered all of the evidence, including the potentially disqualifying and mitigating conditions surrounding this case. Those who know Applicant in the

workplace speak most highly of her. (TR at page 17 line 23 to page 32 line 22, and AppX A, at pages 1~9.) The record evidence leaves me without questions and doubts as to Applicant's eligibility and suitability for a security clearance. For this reason, I conclude Applicant has met her very heavy burden and mitigated the security concerns arising from her Handling of Protected Information, under the whole-person concept.

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
Subparagraph 1.a.	For Applicant
Subparagraph 1.b.	For Applicant
Subparagraph 1.c.	For Applicant
Subparagraph 1.d.	For Applicant
Subparagraph 1.e.	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.

Richard A. Cefola
Administrative Judge