DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 15-05825
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Ray Blank, Esq., Department Counsel
For Applicant: *Pro se*

10/03/2017

Decision

KILMARTIN, Robert J., Administrative Judge:

Applicant mitigated the security concerns under Guideline K (handling protected information). Applicant's eligibility for access to classified information is granted.

Statement of the Case

On April 15, 2016, the Department of Defense (DOD) issued Applicant a Statement of Reasons (SOR) detailing security concerns under Guideline K. Applicant timely answered the SOR and elected to have his case decided on the written record.

Department Counsel submitted the Government's file of relevant material (FORM) on October 5, 2016. Applicant received the FORM on October 13, 2016, and had 30 days to file objections and submit material in refutation, extenuation, or mitigation. Applicant did not object to the Government's evidence, and he provided a two-page response to the FORM dated October 21, 2016. The Government's evidence, identified as Items 1 through 5, is admitted into evidence without objection. The case was assigned to me on September 15, 2017.

Findings of Fact[1]

Applicant is 64 years old. He obtained a master's degree online in 2008 while simultaneously working full time. Applicant has been employed as a physical security officer or site security specialist for a federal contractor since December 2001. Applicant served on active duty in the U.S. Marine Corps for 25 years and received an honorable discharge when he retired in late 2001. He married in 1974 and divorced in 2001, and has been re-married since 2002. He has an adult son and an adult daughter. He has held previous security clearances since 1977 without incident before the transgressions alleged in the SOR.

Applicant disclosed four security violations or infractions that he committed between 2011 and 2014, in section 13A of his 2014 Security Clearance Application (SCA). The earliest violation (SOR ¶ 1.d) occurred when Applicant printed the wrong level of security classification on three visitor badges, which allowed three people to attend a meeting that they were not authorized to attend. He received a written warning. Next, in January 2012 (SOR ¶ 1.c), Applicant received a written warning when he gave classified information to someone who was not authorized to receive it. In December 2013, he received a written reprimand for taking classified material outside of a controlled area (SOR ¶ 1.b). In October 2014, he received a five-day suspension without pay for scanning multiple, classified documents into an unauthorized computer (SOR ¶ 1.a).

In his response to the SOR on May 6, 2016, Applicant admitted all of the allegations in SOR ¶¶ 1.a through 1.d, with explanations. He admitted to printing incorrect clearance levels on three visitors' badges before a short-fused, large meeting in 2011 (SOR ¶ 1.d). All 100 plus visitors were listed on a single visit notification and the higher top secret (TS) clearance personnel were not separated from the lower clearance, secret level personnel. The initial meeting was at the secret level, and a follow-on meeting was at the TS level. All three visitors were properly cleared at the secret level and had a duty to correct the improper classification level on the badges.

Applicant also admitted to handing an employee information that he or she was not cleared to receive (SOR ¶ 1.c). This employee came to the Contract Security Officer (CSO) desk to retrieve his folder. Applicant gave the folder to the employee because it had the employee's name on it. It turned out that the employee was not briefed into the program. This employee bears some responsibility for not alerting Applicant that he was not cleared to receive this folder.

In reference to the December 2013 reprimand alleged at SOR ¶ 1.b, Applicant admits to removing classified information from a controlled area. He reviewed a stack of personnel records before removing them from an inbox that was supposed to contain only unclassified documents. Somebody had inadvertently placed classified documents in this

[1] Unless stated otherwise, the source of the information in this section is Applicant's October 22, 2014 Security Clearance Application (SCA) (Item 4) and his summary of clearance interview by a background investigator dated November 12, 2014 (Item 5).

inbox. These documents were intended to be delivered to different areas and buildings. Security personnel would routinely check the inbox and deliver these documents to whatever building they were going to. The particular document in question must have been stuck to another one, and Applicant did not see it. The person receiving or discovering the errant document, was briefed into the program and immediately returned it to the CSO office. There was no compromise.

.

The most recent allegation (SOR ¶ 1.a) occurred in October 2014 when Applicant admits to receiving a letter of reprimand and five-day suspension without pay for scanning classified documents into a lower-classified computer. The computer was a standalone system, which is only accessible by program personnel who have an authorized user name and password. Applicant was scanning in documents that were not supposed to be classified when he discovered that someone had inadvertently left some classified documents in the pile. This was discovered after Applicant had already scanned them into the computer. He immediately self-reported this incident and the computer in question was scrubbed to remove any classified information. There was no compromise. Applicant contends that the reprimand and suspension were for all of his aggregated security violations, since the contractor has a progressive punishment system

During his clearance interview in November 2014, Applicant stated that with regard to his security violation in SOR ¶ 1.c, he handled thousands of pieces of classified and unclassified documents and materials daily. Applicant stated his intentions to slow down, be more careful and thorough so that he does not make any more errors.[2]

In his October 21, 2016 statement provided in response to the FORM, Applicant states that the Contract Security Office (CSO) has been historically understaffed. The CSO maintains approximately 5,000 personnel records and supports 60 – 80 programs. Applicant handled all visits to program spaces and inputted all visit notifications and visitors' information into the database. On average, he sent by fax approximately 11,000 to 15,000 documents annually. There is no formal training program within the CSO. These four incidents were the product of an inadequate training program in the CSO. Applicant contends that he has learned from his mistakes and he is trustworthy and reliable. As evidence, he points to his recent promotion in January 2016 to the position of Assistant Contract Program Security Officer (ACPSO) in his company.

Policies

DOD took action in this case under Executive Order (EO) 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 (AGs) implemented by DOD on September 1, 2006.

[2] Item 5, p. 4.

On December 10, 2016, the Director of National Intelligence singed Security Executive Agent Directive 4 (SEAD 4), implementing new AGs effective within the DOD on June 8, 2017.[3] Accordingly, I have applied the June 8, 2017 AGs in this decision.

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, 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(a), the adjudicative process is an examination of a sufficient period and a careful weighing of a number of variables of an individual's life to make an affirmative determination that the individual is an acceptable security risk. This is 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 national security eligibility will be resolved in favor of the 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 ¶ 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 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 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.

[3] Although I have decided this case under the adjudicative guidelines (AG) effective June 8, 2017, I also considered the case under the former AG effective on September 1, 2006, and my decision would be the same under either AG.

Section 7 of EO 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 Concern. Deliberate or negligent failure to comply with rules and regulations for handling protected information – which includes classified and other sensitive government information, and proprietary information - raises doubt about an individual's trustworthiness, judgment, reliability, or willingness and ability to safeguard such information, and is a serious security concern.[4]

Security clearance cases require administrative judges to assess whether an applicant has the requisite good judgment, reliability, and trustworthiness to be entrusted with classified information. When evidence is presented that an applicant previously mishandled classified information or violated a rule or regulation for the protection of protected information such an applicant bears a heavy burden in demonstrating that they should once again be found eligible for a security clearance.[5]

Applicant's admitted commission of four security infractions within a three year period raises Guideline K security concerns. In assessing Applicant's case, I considered the following pertinent disqualifying conditions in AG ¶ 34:

> (a): deliberate or negligent disclosure of protected information to unauthorized persons, including, but not limited to, personal or business contacts, the media or persons present at seminars, meetings, or conferences;
>
> (b): collecting or storing protected information in any unauthorized location;
>
> (c): loading, drafting, editing, modifying, storing, transmitting, or otherwise handling protected information, including images, on any unauthorized equipment or medium;
>
> (g): any failure to comply with rules for the protection of classified or other sensitive information; and

[4] AG ¶ 33.

[5] ISCR Case No. 11-12202 at 5 (App. Bd. June 23, 2014) (very heavy burden standard); ISCR Case No. 01-25941 at 5 (App. Bd. May 7, 2004) (security clearance determinations are "not an exact science, but rather predicative judgments.").

(h) negligence or lax security practices that persist despite counseling by management.

I also considered the conditions that could potentially mitigate security concerns including in AG ¶ 35:

> (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 or 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;
>
> (c): the security violations were due to improper or inadequate training or unclear instructions; and
>
> (d): the violation was inadvertent, it was promptly reported, there is no evidence of compromise, and it does not suggest a pattern.

AG ¶ 35(a),(b),(c) and (d) all apply. The security violations were inadvertent and Applicant reported them timely. Sufficient time has passed since his last infraction in 2014 to satisfy me that Applicant is not likely to repeat the same mistakes. In three of the four infractions, other employees were complicit and could have alerted Applicant. Significantly, he has recently been promoted to ACPSO. This is a strong indication of the faith and trust that his employer has in Applicant and his remediation of previous oversights. It demonstrates the company's confidence in his trustworthiness and reliability, and his positive attitude toward the discharge of his security responsibilities. There was no evidence of compromise of classified information. I am confident that Applicant appreciates the significance of his lapses. He has maintained a security clearance for over 40 years. The violations he has admitted were oversights due to lack of conscientious attention to detail, understaffing, and inadequate training. He has improved his focus and vows to be more careful. He voluntarily disclosed these security violations, and he has accepted the reprimands and punishment meted out in each instance. He has met his heavy burden of persuasion.

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(d):

> (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 have incorporated my comments under Guideline K in my whole-person analysis. Some of the factors in AG ¶ 2(d) were addressed under those guidelines. Notably, Applicant has a demonstrated record of 25 years of honorable service in the Marine Corps, and 16 more to federal contractors directly supporting DOD's mission. He has made substantial contributions to military readiness. He has maintained a security clearance for over 40 years. Most importantly, Applicant self-disclosed the specific security violations alleged in the SOR on his SCA. His employer has confidence in his trustworthiness and reliability as evidenced by his recent promotion. He has met his burden of persuasion.

Applicant's multiple admitted security violations no longer remain a security concern. These offenses were minor and they were committed under such unusual circumstances that they are unlikely to recur. There is sufficient evidence to conclude that Applicant has acknowledged the egregiousness of his violations or taken steps to alleviate the stressors or circumstances that contributed his behavior to insure that it does not recur. He has met his burden of persuasion. The record evidence leaves me with no serious questions or doubts as to Applicant's suitability for a security clearance. For all these reasons, I conclude Applicant has mitigated the security concerns arising under Guideline K.

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 through 1.d:	For Applicant

Conclusion

In light of all of the circumstances presented by the record in this case, it is clearly consistent with the interests of national security to grant Applicant a security clearance. Eligibility for access to classified information is granted.

_____
Robert J. Kilmartin
Administrative Judge