DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
----------	)	ISCR Case No. 15-02420
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Candace L. Garcia, Esquire, Department Counsel
For Applicant: *Pro se*

March 27, 2017

_____

Decision

_____

ROSS, Wilford H., Administrative Judge:

On September 11, 2012, Applicant submitted his Electronic Questionnaires for Investigations Processing (e-QIP). (Item 3.) On October 15, 2015, the Department of Defense Consolidated Adjudications Facility (DoD CAF) issued Applicant a Statement of Reasons (SOR) detailing security concerns under Guidelines K (Handling Protected Information) and M (Use of Information Technology Systems). 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 on September 1, 2006.

Applicant answered the SOR in writing on November 12, 2015, and requested his case be decided on the written record in lieu of a hearing. On January 12, 2016, Department Counsel submitted the Department's written case. A complete copy of the

file of relevant material (FORM), consisting of Items 1 to 6, was provided to Applicant, who received the file on February 2, 2016.[1]

Applicant was given 30 days from receipt of the FORM to file objections and submit material in refutation, extenuation, or mitigation. He submitted additional information on March 2, 2016. Department Counsel had no objection and the document is admitted into evidence as Applicant Exhibit A. The case was assigned to me on May 11, 2016. Based upon a review of the pleadings and exhibits, eligibility for access to classified information is granted.

Findings of Fact

Applicant is 58 and married. He is employed by a defense contractor and seeks to obtain a security clearance in connection with his employment.

Paragraph 1 (Guideline K, Handling Protected Information)

The Government alleges in this paragraph that Applicant is ineligible for clearance because he has failed to comply with rules and regulations for protecting classified information. Applicant admitted both allegations in the SOR. He also provided additional information supporting his request for access to classified information.

Applicant has worked for his current employer since 2003. During that time he has had two security violations. They are set forth below:

1.a. On April 10, 2009, Applicant was supposed to close and secure a classified laboratory. He became preoccupied and left without securing the area. In his Answer Applicant states, "After about 45 minutes, and realizing that I forgot to close the lab, I returned immediately to close and set alarm when some of my colleagues were still around at work (in front of the lab), and we confirmed there was one entered the lab during that time. I called and reported [to] security about the incident." (Item 2 at 3.) (*See* Item 5 at 2-5.)

1.b. On July 12, 2012, Applicant sent classified information via an unclassified email system. In addition, he also saved the information on an unclassified server. The next day another employee informed the corporate security office that the subject email

[1] Department Counsel submitted six Items in support of the SOR allegations. Item 4 is inadmissible. It will not be considered or cited as evidence in this case. It is the summary of an unsworn interview of Applicant conducted by an interviewer from the Office of Personnel Management on January 30, 2013. Applicant did not adopt the summary as his own statement, or otherwise certify it to be accurate. Under Directive ¶ E3.1.20, this Report of Investigation summary is inadmissible in the absence of an authenticating witness. In light of Applicant's admissions, and other evidence in the record, it is also cumulative.

contained classified information. The email was sent to 27 people, some of whom worked for a different company. According to corporate security, "[Applicant] stated that he was in a hurry to complete his report . . . and forgot that the data was classified." Applicant received a written memorandum, entitled "Employee Corrective Action Memo," on August 10, 2012, regarding this incident. (Item 5 at 1, 5-16.)

Paragraph 2 (Guideline M, Use of Information Technology Systems)

The Government alleges in this paragraph that the Applicant's conduct set forth under Paragraph 1, above, showed noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems. Applicant admitted this allegation.

With regard to the above incidents he states in Applicant Exhibit A:

> With all due respect, throughout my 33 years working for U.S. Department of Defense . . ., I have never had malicious or deliberate intention to abuse rules or regulations for protecting classified information. I am regretful that these past 2 unfortunate security breaches occurred under my negligence. I admit to making an honest mistake and will sincerely take appropriate steps to prevent any future infractions or violations. . . . I have had no infractions for almost 4 years since the last incident in July 2012. I truly take pride in my work and will strive to be more conscientious with sensitive material.

Applicant submitted no other information concerning the quality of his work. He submitted no character references or other evidence tending to establish good judgment, trustworthiness, or reliability. I was unable to evaluate his credibility, demeanor, or character in person since he elected to have his case decided without a hearing.

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, the administrative judge applies the guidelines in conjunction with the factors listed in AG ¶ 2 describing 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, "Any 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.

According to Directive ¶ E3.1.14, the Government must present evidence to establish controverted facts alleged in the SOR. Under Directive ¶ E3.1.15, "The applicant is responsible for presenting witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by the applicant or proven by Department Counsel, and has the ultimate burden of persuasion as to obtaining a favorable clearance 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.

Finally, as emphasized in Section 7 of Executive Order 10865, "Any determination under this order adverse to an applicant shall be a determination 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

Paragraph 1 (Guideline K - Handling Protected Information)

The security concern relating to Handling Protected Information is set out in AG ¶ 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, judgment, reliability, or willingness and ability to safeguard such information, and is a serious security concern.

I have considered the disqualifying conditions under AG ¶ 34 and especially considered the following:

> (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.

I have also considered the mitigating conditions under AG ¶ 35 and especially considered the following:

> (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.

Paragraph 2 (Guideline M - Use of Information Technology Systems)

The security concern relating to the guideline for Use of Information Technology Systems is set out in AG ¶ 39:

> Noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual's reliability 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.

I have examined the disqualifying conditions under AG ¶ 40 and especially considered the following:

> (d) downloading, storing, or transmitting classified information on or to any unauthorized software, hardware, or information technology system; and
>
> (e) unauthorized use of a government or other information technology system.

I have also considered the mitigating conditions under AG ¶ 41 and especially considered the following:

> (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 failed to properly secure a classified laboratory in 2009. For this incident he received a security infraction. In 2012 he sent classified information over an unclassified email system, and also stored the same information on an unclassified computer system. This latter incident was viewed more seriously, as a security violation. He received counseling from his employer for both incidents. The facts are sufficient to support the allegations under each paragraph of the SOR, requiring Applicant to present sufficient evidence to mitigate the security significance of those facts.

Applicant has had no further security-related incidents in the four years since the second incident. The amount of time since an incident happened is viewed as a mitigating condition under both Guideline K and Guideline M. In addition, he forthrightly admitted his responsibility for each security violation, and did not attempt to excuse it or blame someone else. Under the particular circumstances of this case, I find that four years is a sufficient time to show that the conduct is unlikely to recur and does not cast doubt on Applicant's reliability, trustworthiness, or good judgment. Paragraphs 1 and 2 are found for Applicant.

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 relevant 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 facts and circumstances surrounding this case. Applicant's security violations, which also consisted of misuse of information technology systems, are now remote in time and have not been repeated. Overall, the record evidence as described above leaves me without questions or doubts as to Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude Applicant did mitigate the security concerns arising under the guidelines for Handling Protected Information, and Use of Information Technology Systems.

Formal Findings

Formal findings for or against Applicant on the allegations set forth in the SOR, as required by ¶ E3.1.25 of Enclosure 3 of the Directive, are:

Paragraph 1, Guideline K:	FOR APPLICANT
Subparagraphs 1.a and 1.b:	For Applicant
Paragraph 2, Guideline M:	FOR APPLICANT
Subparagraph 2.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.

WILFORD H. ROSS
Administrative Judge