DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 16-01333
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Pamela Benson, Esq., Department Counsel
For Applicant: Leonard L Casalino, Esq.

11/17/2017

_____

Decision

_____

Curry, Marc E., Administrative Judge:

Applicant mitigated the security concerns under Guideline K, handling protected information, and Guideline E, personal conduct. Clearance is granted.

Statement of the Case

On November 9, 2016, the Department of Defense Consolidated Adjudications Facility (DOD CAF) issued a Statement of Reasons (SOR) to Applicant, detailing the security concerns under Guidelines K, handling protected information, and E, personal conduct, explaining why it was unable to find it clearly consistent with the national interest to grant security clearance eligibility for him. The DOD CAF took the action 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 for Determining Eligibility for Access to Classified Information* (AG) effective within the DOD on September 1, 2006.

On December 14, 2016, Applicant answered the SOR allegations, admitting all of the allegations, and requested a decision based on the written record instead of a hearing.

On November 9, 2016, Department Counsel prepared a File of Relevant Material (FORM). Applicant received the FORM on April 15, 2017. He then retained an attorney and filed a response on May 11, 2017. The case was assigned to me on October 1, 2017.

While this case was pending a decision, Security Executive Agent Directive 4 was issued establishing National Security Adjudicative Guidelines (AG) applicable to all covered individuals who require initial or continued eligibility for access to classified information or eligibility to hold a sensitive position. The AG supersede the adjudicative guidelines implemented in September 2006 and are effective for any adjudication made on or after June 8, 2017. Accordingly, I have adjudicated Applicant's security clearance eligibility under the new AG.

Evidentiary Ruling

Item 3 is a Report of Investigation (ROI) summarizing Applicant's Personal Subject Interviews conducted on October 21, 2015 and March 8, 2016. Such reports are typically inadmissible without authenticating witnesses. Directive ¶ E3.1.20**.** Applicant's counsel, however, did not object to the inclusion of the interview summaries in the FORM, and he referenced them in his response. Consequently, I have incorporated the interview summaries into the record and have considered them in my disposition of the case.

Findings of Fact

Applicant is a 64-year-old married man. He earned a bachelor's degree in 1977 and an information technology certificate in 1987. He has worked in the network administration field for various defense contractors for the past 25 years. During this time, he has held a security clearance. Since 1999, he has worked in the position of principal network administrator. (Item 1 at 36)

Applicant is highly respected on the job. In 2008, the division chief of the agency that Applicant supported wrote a letter of commendation to Applicant's company, informing them that Applicant had "excelled far beyond rightful expectations for his position." (Item 1 at 8) In addition, he commended Applicant for the "continuous outstanding support" that he had been providing over the years. (Item 1 at 12) He particularly noted Applicant's ability to exceed at a high level, performing under the "severe scrutiny" of the information technology security office and working promptly while navigating "the many stringent requirements due to perpetually growing information technology security rules and regulations." (Item 1 at 12) In 2011, the division chief again contacted Applicant's employer to complement his performance, noting that the division had "come to expect consistently excellent support from Applicant, but he had "exceeded even those high expectations." (Item 1 at 14) During an office move, Applicant "ensured that the computing systems classified network . . . was up and operational, with full functionality, with minimal downtime . . . despite an unexpected reduction of time for installation and test from a planned 30 days to just seven." (Item 1 at 14)

One Friday evening May 12, 2015, Applicant inadvertently placed four pages of information, printed from a classified printer, into his notebook and took them home over the weekend. (Item 3 at 4; Response at 4) He discovered this mistake when he prepared to do some work at home and opened the notebook. He then removed the papers and placed them into his laptop computer bag compartment. When Applicant returned to work on May 15, 2016, he shredded the four pages, then e-mailed the agency's information assurance officer. On May 19, 2015, he notified his supervisor and the agency division chief where he was assigned. (Response at 5; Item 3 at 4)

When Applicant contacted the agency division chief, he also disclosed a previous incident that occurred in 2014 when he was conducting a printer test to ensure that his work laptop was connected to the printer. When he was finished running the test, he accidentally left the printer connection test page, identifying that the printer was classified, in his laptop when he closed the laptop. Both classified and unclassified information could be received from this printer. (Item 3 at 5) Applicant did not realize what he had done until he took the laptop home and opened it. (Item 3 at 6) When he discovered the error, he immediately returned the test page to work and shredded it. (Item 3 at 6)

The agency division chief and the agency facility security officer (FSO) contacted Applicant and told him that any ensuing internal investigation would focus solely on the May 2015 incident. (Response at 4-5) Then, Applicant's FSO contacted him on May 27, 2015 and instructed him to complete an online security clearance application. On June 1, 2015, Applicant completed the form, as instructed. (Item 2) In response to Section 27, Question 1 "in the last seven years have you introduced, removed, or used hardware, software, or media in connection with any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines, or regulation or attempted any of the above?" he answered "yes," and discussed the 2015 incident, but omitted the 2014 incident.

Applicant did not discuss the 2014 incident when an investigative agent interviewed him in October 2014. (Item 1 at 3) He thought he did not need to discuss the 2014 incident because the agency chief and the agency FSO had told him that any internal investigation would focus solely on the May 2015 incident. (Response at 4**)** During Applicant's first investigative interview, he gave the agent the contact information of his supervisor and the company's FSO. (Response at 6) In addition, after the first interview, he told his supervisor that the investigator would probably contact her. (Response at 6)

On June 18, 2015, Applicant received an e-mail from his company's FSO who informed him that he was going to be verbally counseled for the 2015 incident and required to retake the company's initial security briefing and information directives, together with a security refresher training. (Response at 5-6) He successfully completed the training. (Response at 10)

Policies

The U.S. Supreme Court has recognized the substantial discretion the Executive Branch has in regulating access to information pertaining to national security, emphasizing that "no one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988). 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 required to be considered 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 overall adjudicative goal is a fair, impartial, and commonsense decision. 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, 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 to obtain a favorable security decision.

Under the whole-person concept, the administrative judge must consider the totality of an applicant's conduct and all relevant circumstances in light of the nine adjudicative process factors in AG ¶ 2(d).[1]

[1] The factors under AG ¶ 2(d) are as follows:

> (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.

Analysis

Guideline K, Handling Protected Information

Under this guideline, "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." (AG ¶ 33) Applicant's security violations in 2014 and 2015 trigger the application of AG ¶ 34(g), "any failure to comply with rules for the protection of classified information."

The incidents that form the basis of the SOR were both unintentional. In addition, they are the only violations that Applicant has committed in the 25 years that he has held a security clearance. Historically, Applicant has been exceptional at balancing security consciousness with work performance, as noted in two commendation letters. Under these circumstances, AG ¶ 35(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," applies.

After the 2015 security violation, Applicant received security awareness counseling and completed a remedial security awareness briefing. The first prong of AG ¶ 35(b), "the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities," applies.[2]

Security violations represent significant misconduct. As the Appeal Board noted, they "are one of the strongest possible reasons for denying or revoking access to classified information, as they raise serious questions about an applicant's suitability for access to classified information." (ISCR Case No. 01-24358 at 4 (App. Bd. Apr. 13, 2004)). Nevertheless, the nature and seriousness of the security violations must still be weighed against the mitigating factors. Here, the negative ramifications of the security violations are outweighed by the infrequent nature of the conduct, the presence of rehabilitation, Applicant's history of exceptional security consciousness, and his stellar work performance, rendering the likelihood of recurrence minimal. In sum, Applicant has mitigated the Guideline K security concern.

Guideline E, Personal Conduct

Under this guideline, "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 or sensitive information." Moreover, "of special interest is any failure to cooperate or provide truthful

[2]The second prong of AG ¶ 35(b) is not relevant because there is no record evidence that Applicant ever had a negative attitude toward the discharge of his security responsibilities.

and candid answers during national security investigative or adjudicative processes." (AG ¶ 15) Applicant's failure to disclose the 2014 security episode to the investigator who interviewed him in October 2015 raises the issue of whether AG ¶ 16(b), "deliberately providing false or misleading information; or concealing or omitting information, concerning relevant facts to an employer, investigator, security official, competent medical or mental health professional involved in making a recommendation relevant to a national security eligibility determination, or other official government representative," applies. Applicant self-reported both security violations. He thought that he did not need to address the 2014 incident because both the agency chief and the agency FSO had told him that any internal investigation would focus solely on the May 2015 incident. (Response at 4**)** Moreover, although he did not disclose the 2014 incident to the agent when asked about previous security violation, he gave the agent the contact information of his supervisor and the company's FSO, and told his supervisor that the investigative agent would probably contact her. Under these circumstances, I conclude that Applicant did not intend to mislead the investigator, and that there are no personal conduct security concerns.

Whole-Person Concept

I considered the whole-person factors in my analysis of the disqualifying and mitigating conditions, particularly when gauging Applicant's credibility.

Formal Findings

Formal findings for 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 E:	FOR APPLICANT
Subparagraphs 2.a – 2.b:	For Applicant

Conclusion

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

_____
Marc E. Curry
Administrative Judge