DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
------	)	ISCR Case No. 14-00053
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Eric Borgstrom, Esquire, Department Counsel
For Applicant: *Pro se*

01/21/2015

Decision

GALES, Robert Robinson, Administrative Judge:

Applicant mitigated the security concerns regarding handling protected information and personal conduct. Eligibility for a security clearance and access to classified information is granted.

Statement of the Case

On May 22, 2002, Applicant applied for a security clearance and submitted a Security Clearance Application (SF 86).[1] On February 18, 2008, Applicant submitted another Security Clearance Application (2nd SF 86).[2] On May 3, 2013, he submitted an Electronic Questionnaire for Investigations Processing (e-QIP) version of a Security Clearance Application.[3] On March 21, 2014, the Department of Defense (DOD) Consolidated Adjudications Facility – Division A (CAF) issued him a Statement of Reasons (SOR), under Executive Order 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended and modified; DOD Directive 5220.6,

[1] Item 5 (SF 86, dated May 22 18, 2002).

[2] Item 4 (SF 86, dated February 18, 2008).

[3] Item 3 (e-QIP), dated May 3, 2013).

Defense Industrial Personnel Security Clearance Review Program (January 2, 1992), as amended and modified (Directive); and the *Adjudicative Guidelines for Determining Eligibility For Access to Classified Information* (December 29, 2005) (AG) applicable to all adjudications and other determinations made under the Directive, effective September 1, 2006. The SOR alleged security concerns under Guideline K (Handling Protected Information) and Guideline E (Personal Conduct), and detailed reasons why the DOD adjudicators were unable to find that it is clearly consistent with the national interest to grant or continue a security clearance for Applicant. The SOR recommended referral to an administrative judge to determine whether a clearance should be granted, continued, denied, or revoked.

It is unclear when Applicant received the SOR as there is no receipt in the case file. In a statement notarized April 15, 2014, Applicant responded to the SOR allegations, and elected to have his case decided on the written record in lieu of a hearing.[4] A complete copy of the Government's file of relevant material (FORM) was prepared by the Defense Office of Hearings and Appeals (DOHA). The FORM was provided to Applicant on November 5, 2014, and he was afforded an opportunity, within a period of 30 days after receipt of the FORM, to file objections and submit material in refutation, extenuation, or mitigation. Applicant received the FORM on November 14, 2014. Applicant responded to the FORM, and on December 11, 2014, he submitted additional documentation. The case was assigned to me on January 5, 2015.

Findings of Fact

In his Answer to the SOR, Applicant admitted the factual allegations in the SOR pertaining to handling protected information (¶¶ 1.a. through 1.d.). He failed to address the allegation pertaining to personal conduct (¶ 2.a.). Applicant's admissions are incorporated herein as findings of fact. After a complete and thorough review of the evidence in the record, and upon due consideration of same, I make the following additional findings of fact:

Applicant is a 64-year-old employee of a defense contractor, and he is seeking to retain the top secret security clearance that he was initially granted in September 1984.[5] In September 2003, He was also granted access to sensitive compartmented information (SCI) at that time. That SCI access was periodically renewed,[6] but it is not known if he still has such access. He has been employed by the same defense contractor as a research assistant since February 2000,[7] and previously worked for another federal contractor for 16 years. He has never served with the United States military.[8]

[4] Item 2 (Applicant's Answer to the SOR).

[5] Item 6 (Personal Subject Interview, dated August 23, 2013), at 3; Item 5, *supra* note 1, at 33; Item 4, *supra* note 2, at 7; Item 3, *supra* note 3, at 29-30.

[6] Item 6, *supra* note 5, at 3; Item 4, *supra* note 2, at 7.

[7] Item 3, *supra* note 3, at 12.

[8] Item 3, *supra* note 3, at 14.

A 1968 high school graduate,[9] Applicant received a bachelor's degree in 1972 and master's degrees in 1975 and 1990.[10] Applicant was married in 1975, and he and his wife have two adult children: a daughter (born in 1981) and a son (born in 1984).[11]

Handling Protected Information & Personal Conduct

(SOR ¶¶ 1.d. and 2.a.): In February 2003, after working within a closed area containing an outer room and an inner room (containing closed storage of classified material), Applicant fully engaged the security measures of the inner room, but failed to engage all of the supplemental protection security measures of the outer room. The alarm was activated, but he failed to engage the locking mechanism. An investigation conducted by the facility security officer (FSO) concluded that there was no compromise or attempted compromise of classified material because one of the supplemental protection security measures was functional and there were no signs of attempted entry or missing items.[12] While Applicant admitted that the incident constituted a "security violation,"[13] in fact, under DOD 5220.22-M-Sup, *National Industrial Security Program Operating Manual Supplement* (February 1995), it should have been classified as a "security infraction."[14]

(SOR ¶¶ 1.c. and 2.a.): Seven years later, in October 2010, after working within the same closed area with a cleared colleague, Applicant failed to lock the security container assigned to him within the inner room and failed to engage the locking mechanism of the inner room. He did, however, activate the alarm of the inner room, as well as engage all of the supplemental protection security measures of the outer room. An investigation conducted by the FSO concluded that there was no compromise or attempted compromise of classified material because the supplemental protection security measures of the outer room were functional and there were no signs of attempted entry or missing items.[15] The incident should have been classified as a "security infraction."

(SOR ¶¶ 1.b. and 2.a.): In February 2011, while working in the same outer room, Applicant replaced a 5-disc compact disc (CD) player used to generate "white noise" with a single disc player. He removed the five unclassified CDs contained in the CD

---

[9] Item 3, *supra* note 3, at 9-10.

[10] Item 3, *supra* note 3, at 10-11.

[11] Item 3, *supra* note 3, at 22-23.

[12] Item 2, *supra* note 4, at 3.

[13] Item 2, *supra* note 4, at 3. "A security violation is any incident that involves the loss, compromise, or suspected compromise of classified information." DOD 5220.22-M-Sup, § 1-301.a. (1).

[14] "A security infraction is any other incident that is not in the best interest of security that does not involve the loss, compromise, or suspected compromise of classified information." DOD 5220.22-M-Sup, § 1-301.a. (2).

[15] Letter from FSO, dated October 26, 2010, attached to Item 2.

player and placed the remaining four CDs on the shelf adjacent to the disc player. Each of the CDs was already in the closed area and labeled in compliance with the instructions previously furnished. In that area, a green mark indicated "unclassified." The entire word was not used because it was office policy and the closed area network plan not to do so. The policy and plan eventually evolved into a lab-wide plan which apparently mandated the use of the entire word. The green markings on the CDs should have been modified by someone, not identified, but they were not. During a normal security patrol, the guard noticed the CDs and confiscated them. An investigation conducted by the FSO concluded that there was no compromise or attempted compromise of classified material because the supplemental protection security measures of the outer room were functional and there were no signs of attempted entry or missing items.[16] The incident was classified as a "minor incident" by the FSO, and Applicant was issued a verbal warning.[17]

(SOR ¶¶ 1.a. and 2.a.): In May 2012, after working within the same inner room, Applicant engaged the locking mechanism of the room, but failed to activate the alarm of the room. While the outer room was no longer a closed area, he did engage all of the supplemental protection security measures of the outer room. An investigation conducted by the FSO concluded that there was no compromise or attempted compromise of classified material because the supplemental protection security measures of the outer room were functional and there were no signs of attempted entry or missing items.[18] Applicant received a written notification for the incident and advised to review and follow all the procedural steps on the closed area instruction sheet.[19] The incident should have been classified as a "security infraction." Following the May 2012 incident, Applicant was advised by the FSO that if any future issues such as the latest one should occur, and if they suggest a pattern of recklessness with security requirements or deliberate disregard, the FSO would be required to file an adverse action report to the Defense Security Service pursuant to § 1-304, DOD 5220.22-M, *National Industrial Security Program Operating Manual* (February 2006) (NISPOM).

The Security Manager for SCI and Special Programs noted that since Applicant's indoctrination for SCI in 2006, Applicant attended yearly SCI security refresher training, and he has not received any written warnings for practices dangerous to security or violations within the SCIF areas.[20] The FSO noted that Applicant "expressed his contrition for the incidents and made tangible efforts to avoid repeating the lapses involved by increasing his level of vigilance."[21] Applicant has acknowledged that he was careless when he failed to complete the various security protocols that had been

[16] Letter from FSO, dated October 26, 2010, attached to Item 2; Security Incident Report, dated February 7, 2011, attached to Item 2.

[17] Letter from FSO, dated April 13, 2014, at 1, attached to Item 2; Security Incident Report, supra *note* 16.

[18] Letter from FSO, dated May 11, 2012, attached to Item 2.

[19] Letter from FSO, *supra* note 18.

[20] Letter from Security Manager for SCI and Special Programs, dated April 3, 2014, attached to Item 2.

[21] Letter from FSO, *supra* note 17, at 2.

established, and he has since taken a variety of steps to insure that his inadvertent failures do not recur. He has reminders pop up on his computer screen at work; he placed a sign over the locking mechanism of the doors; and he placed a checklist on the inner room door on which he notes the time opened, time closed, alarm activated, and door locked.[22]

Character References

Applicant's immediate supervisor, who has known and worked with Applicant for over 25 years, and is the individual who initially hired him, is highly supportive of Applicant's application. He has no reservations regarding Applicant's commitment to support the rules and regulations for protecting classified information.[23] The FSO has known Applicant for about four years, and he has referred to Applicant as having distinguished himself as an honest and hardworking researcher who understands the importance of security policies and procedures to protect classified material with which he is entrusted. The FSO cited Applicant's integrity and candor as being exemplified by his listing more security incidents in his e-QIP than were actually required. Only two of the incidents should have been listed, neither of which risked the compromise of classified material.[24] The FSO concluded that neither incident resulted from deliberate disregard, gross negligence or a pattern of negligence under the NISPOM.[25] The FSO recommends, without reservation, that Applicant retain his security clearance.[26]

Policies

The U.S. Supreme Court has recognized the substantial discretion of the Executive Branch in regulating access to information pertaining to national security emphasizing, "no one has a 'right' to a security clearance."[27] As Commander in Chief, the President has the authority to control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to have access to such information. The President has authorized the Secretary of Defense or his designee to grant an applicant's eligibility for access to classified information "only upon a finding that it is clearly consistent with the national interest to do so."[28]

When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the adjudicative guidelines. In addition to brief

[22] Item 6, *supra* note 5, at 2; Item 2, *supra* note 4, a t3-4.

[23] Character Reference, dated April 14, 2014, attached to Item 2.

[24] Letter from FSO, *supra* note 17, at 1-2.

[25] Letter from FSO, *supra* note 17, at 2.

[26] Letter from FSO, *supra* note 17, at 2.

[27] *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988).

[28] Exec. Or. 10865, *Safeguarding Classified Information within Industry* § 2 (Feb. 20, 1960), as amended and modified.

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.

An administrative judge need not view the guidelines as inflexible, ironclad rules of law. Instead, acknowledging the complexities of human behavior, these guidelines are applied in conjunction with the factors listed in the adjudicative process. The administrative judge's over-arching adjudicative goal is a fair, impartial and common sense decision. 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 meaningful decision.

In the decision-making process, facts must be established by "substantial evidence."[29] The Government initially has the burden of producing evidence to establish a potentially disqualifying condition under the Directive, and has the burden of establishing controverted facts alleged in the SOR. Once the Government has produced substantial evidence of a disqualifying condition, under Directive ¶ E3.1.15, the applicant has the burden of persuasion to present evidence in refutation, explanation, extenuation or mitigation, sufficient to overcome the doubts raised by the Government's case. The burden of disproving a mitigating condition never shifts to the Government.[30]

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 as well. It is because of this special relationship that the Government must be able to repose a high degree of trust and confidence in those 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. Furthermore, "security clearance determinations should err, if they must, on the side of denials."[31]

Clearance decisions must be "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned."[32] Thus, nothing in this decision should be construed to suggest that I have based this decision, in whole or in part, on any express or implied determination as to Applicant's allegiance, loyalty,

[29] "Substantial evidence [is] such relevant evidence as a reasonable mind might accept as adequate to support a conclusion in light of all contrary evidence in the record." ISCR Case No. 04-11463 at 2 (App. Bd. Aug. 4, 2006) (citing Directive ¶ E3.1.32.1). "Substantial evidence" is "more than a scintilla but less than a preponderance." *See v. Washington Metro. Area Transit Auth.*, 36 F.3d 375, 380 (4th Cir. 1994).

[30] *See* ISCR Case No. 02-31154 at 5 (App. Bd. Sep. 22, 2005).

[31] *Egan*, 484 U.S. at 531

[32] *See* Exec. Or. 10865 § 7.

or patriotism. It is merely an indication the Applicant has not met the strict guidelines the President and the Secretary of Defense have established for issuing a clearance. 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.

Analysis

Guideline K, Handling Protected Information

The security concern relating to the guideline for 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.

The guideline notes a condition that could raise security concerns. Under AG ¶ 34(g) "any failure to comply with rules for the protection of classified or other sensitive information*"* is potentially disqualifying. In addition, "negligence or lax security habits that persist despite counseling by management" may raise security concerns under AG ¶ 34(h). Applicant's employer determined that his actions in 2003, 2010, 2011, and 2012, violated various security policies and procedures. Most of those incidents constituted "security infractions," and none of them constituted "security violations" under the NISPOM Supplement. Nevertheless, AG ¶¶ 34(g) and 34(h) have been established.

The guideline also includes examples of conditions that could mitigate security concerns arising from handling protected information. Under AG ¶ 35(a), the disqualifying condition may be mitigated where "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.*"* Also, AG ¶ 35(b) may apply if "the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities." Applicant has had four security incidents in nine years in the 30-year period during which he has held a top secret security clearance. Three of the security infractions involved his failure to activate or engage all of the supplemental protection security measures available in the security system. One incident involved unclassified CDs that were not properly marked as such.

After conducting security investigations for each of the cited incidents, the FSO concluded that there was no compromise or attempted compromise of classified material because most of the supplemental protection security measures were engaged or activated and functional, and there were no signs of attempted entry or missing items. After disregarding the continuing significance of the incidents of 2003 and 2011, the FSO also concluded that neither of the remaining incidents resulted from deliberate

disregard, gross negligence or a pattern of negligence under the NISPOM. I found Applicant's evidence, including his statements and those of the FSO and the Security Manager for SCI and Special Programs, to be consistent and credible.

The most recent security incident – a security infraction – when Applicant engaged the locking mechanism of the inner room, but failed to activate the alarm of that room, occurred in May 2012, approximately two and one-half years before the date of the hearing. Applicant attended yearly SCI security refresher training, and he has not received any written warnings for practices dangerous to security or violations within the SCIF areas.

Furthermore, Applicant expressed his contrition for the incidents and made tangible efforts to avoid repeating the lapses involved by increasing his level of vigilance. Applicant has acknowledged that he was careless and has taken a variety of steps to insure that his inadvertent failures do not recur. While there are these four incidents, Applicant has, nevertheless, demonstrated a positive attitude to the discharge of his security responsibilities and embraced security consciousness. Considering the totality of the evidence, I find that AG ¶¶ 35(a) and 35(b) apply to mitigate the security concerns.

Guideline E, Personal Conduct

The security concern relating to the guideline for Personal Conduct is set out in AG ¶ 15:

> 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.

The guideline notes a condition that could raise security concerns. Under AG ¶ 16(d), it is potentially disqualifying if there is

> credible adverse information that is not explicitly covered under any other guideline and may not be sufficient by itself for an adverse determination, but which, when combined with all available information 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. This includes but is not limited to consideration of: . . . (3) a pattern of dishonesty or rule violations. . . .

Applicant's employer determined that Applicant's actions in 2003, 2010, 2011, and 2012, violated various security policies and procedures. That is four security incidents in the 30-year period during which he has held a top secret security clearance.

Most of those incidents constituted "security infractions," and none of them constituted "security violations" under the NISPOM Supplement. The FSO concluded that there was no deliberate disregard, gross negligence or a pattern of negligence under the NISPOM, and recommends, without reservation, that Applicant retain his security clearance. Nevertheless, AG ¶ 16(d) has been established.

The guideline also includes examples of conditions that could mitigate security concerns arising from personal conduct. If "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," AG ¶ 17(c) may apply. Also, AG ¶ 17(d) may apply if "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*."* Similarly, AG ¶ 17(e) may apply if "the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress*."*

The FSO noted that Applicant expressed his contrition for the incidents and made tangible efforts to avoid repeating the lapses involved by increasing his level of vigilance. Applicant acknowledged that he was careless when he failed to complete the various security protocols that had been established, and he has taken a variety of steps to insure that his inadvertent failures do not recur. A person should not be defined by, or held forever accountable for, isolated incidents of poor judgment from the past, especially if there is a clear indication of subsequent reform, remorse, or rehabilitation. Applicant's security clearance has been periodically renewed over a 30-year period. He has not been involved in another security incident in two and one-half years. AG ¶¶ 17(c), 17(d), and 17(e) apply. I conclude that Applicant's actions no longer cast doubt on his reliability, trustworthiness, or good judgment.

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. Moreover, I have evaluated the various aspects of this case in light of the totality of the record evidence and have not merely performed a piecemeal analysis.[33]

There is some evidence against mitigating Applicant's handling of protected information and personal conduct. During a nine-year period, in 2003, 2010, 2011, and 2012, he violated various security policies and procedures.

The mitigating evidence under the whole-person concept is more substantial. Applicant has held a top secret security clearance, sometimes with access to SCI, for 30 years. Three of the security infractions involved his failure to activate or engage all of the supplemental protection security measures available in the security system. One incident involved unclassified CDs that were not properly marked as such. After conducting security investigations for each of the incidents, the FSO concluded that there was no compromise or attempted compromise of classified material because most of the supplemental protection security measures were engaged or activated and functional, and there were no signs of attempted entry or missing items. Applicant expressed his contrition for the incidents and made tangible efforts to avoid repeating the lapses involved by increasing his level of vigilance. Overall, the record evidence leaves me without questions and doubts as to Applicant's eligibility and suitability for a security clearance. After weighing the disqualifying and mitigating conditions, and all the facts and circumstances, in the context of the whole person, I conclude he has mitigated and overcome the Government's case. *See* AG ¶ 2(a)(1) through AG ¶ 2(a)(9).

I take this position based on the law, as set forth in *Department of Navy v. Egan,* 484 U.S. 518 (1988), my careful consideration of the whole-person factors and supporting evidence, my application of the pertinent factors under the adjudicative process, and my interpretation of my responsibilities under the Guidelines. For the reasons stated, I conclude he is eligible for access to classified information.

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

[33] *See U.S. v. Bottone*, 365 F.2d 389, 392 (2d Cir. 1966); *See also* ISCR Case No. 03-22861 at 2-3 (App. Bd. Jun. 2, 2006).

Paragraph 2, Guideline E: 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 national security to grant Applicant eligibility for a security clearance. Eligibility for access to classified information is granted.

_____
ROBERT ROBINSON GALES
Administrative Judge