DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 16-03861
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Mary Margaret Foreman, Esq., Department Counsel
For Applicant: Krista Wallace, Esq.

07/06/2018

_____

Decision

_____

CERVI, Gregg A., Administrative Judge

This case involves security concerns raised under Guideline K (Handling Protected Information) and Guideline E (Personal Conduct). Eligibility for access to classified information is denied.

Statement of the Case

Applicant submitted a security clearance application (SCA) on August 10, 2015. On April 28, 2017, the Department of Defense Consolidated Adjudications Facility (DOD CAF) sent him a Statement of Reasons (SOR) alleging security concerns under Guidelines K and E. Applicant responded to the SOR on May 24, 2017, and requested a hearing before an administrative judge.[1] Department Counsel made minor amendments to SOR ¶ 1.a on July 19, 2017, that Applicant acknowledged without objection on July 25, 2017.

[1] The DOD CAF acted under Executive Order (Exec. Or.) 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 (AG) implemented by the DOD on September 1, 2006. These guidelines were revised on June 8, 2017, and are applicable to all decisions issued thereafter.

The case was assigned to me on August 9, 2017. Defense Office of Hearings and Appeals (DOHA) issued a notice of hearing on October 13, 2017, scheduling the hearing for November 16, 2017. Applicant requested a continuance of the hearing to permit him time to retain counsel. After coordination with counsel, DOHA issued a second notice of hearing on February 8, 2018, scheduling the hearing for February 26, 2018. The hearing was convened as scheduled. Government Exhibits (GE) 1 through 4 were admitted in evidence without objection. Applicant testified and Applicant's Exhibits (AE) A and B were admitted without objection. The record was held open for Applicant to submit additional information, however he declined to supplement the record. DOHA received the hearing transcript (Tr.) on March 5, 2018.

Findings of Fact

Applicant is a 60-year-old information systems security analyst for a defense contractor, employed since 2015. He worked for another defense contractor from 1993 to 2015. Applicant honorably served in the U.S. Navy from 1977 to 1985. He was married and divorced twice; the last marriage was in 1991 and he divorced in 2003. He has one adult child. Applicant was awarded a bachelor's degree in information technology in 2007 and a master's degree in business administration in 2009. He is currently living with a cohabitant, and has held a security clearance for more than 10 years.

The SOR alleges Applicant had various security violations while working for his previous employer. In addition, the SOR alleges Applicant failed to disclose a 2015 incident resulting in an employee corrective action memo (CAM), in his SCA and during a personal security interview (PSI) by a Government investigator. Applicant admitted SOR ¶¶ 1.a - 1.c, but denied ¶¶ 1.d and 2.a – 2.c. In general, Applicant disputes the facts underlying the 2015 incident alleged in ¶ 1.d, and disputes whether he was required to report it in his SCA, and during the PSI, claiming there was a miscommunication with the investigator.

In 2012, Applicant failed to properly secure a document containing classified information. The document was a training package that he was required to use to brief new employees on marking and handling classified material. After a co-worker notified him that the document contained classified information, Applicant again failed to secure it in the safe. Instead, he locked it in a desk drawer. Applicant claimed it was improperly marked and he did not realize it contained a classified page, but acknowledged that he was responsible for ensuring it was properly handled and safeguarded. He was verbally warned.

In 2014, Applicant received a verbal warning for improperly posting a document containing special handling instructions on an unclassified computer share drive. Applicant does not recall putting the document on the unclassified system. Again, in 2014, Applicant improperly scanned and emailed classified material on an unclassified system to a government customer. The customer reported the incident to Applicant's employer, and Applicant received a CAM. Applicant acknowledged that he should have marked the document as classified and should not have sent it on an unclassified system.

Finally, in 2015, Applicant received a CAM for falsifying documents claiming to have completed tasks assigned to him and for altering paperwork related to those tasks that he falsely attested to completing. Applicant argues that he had limited access to the space in question, and could only certify inspecting the material to which he had access. However, it appears that he certified that all inspections were completed without explaining that he had limited access. The 2015 incident occurred about one month before Applicant's departure from the company, but was not recorded in a CAM until the day he left. Applicant noted that he believed the security program manager that initiated the CAM was retaliating for previous reports he made to human resources about her,[2] and her hostility to him.[3]

When reapplying for a security clearance in 2015, Applicant was concerned about whether he had to report the 2015 CAM in his SCA. He consulted his new employer and coworkers for advice. He argues that he did not have to report the 2015 CAM based on advice from his new security manager. He acknowledges that he did not show her the CAM, but described the incidents to her. The security manager acknowledged that she did not see the CAM and does not recall the details of the discussion with Applicant. Applicant omitted the 2015 incident in his SCA, and when the opportunity arose to discuss it with a Government investigator during his PSI, Applicant failed to voluntarily disclose it. Applicant believes it was a misunderstanding between him and the investigator.

Applicant provided a letter of support from a colleague, who attested to Applicant's integrity and character. Although Applicant answered all questions while testifying, he often shifted responsibility for the SOR incidents to the actions of others, technical issues, or changes to regulations and procedures. There is no evidence that his security violations were intentional. Rather, the evidence suggests Applicant's actions resulted from a negligent lack of security awareness and inattention to detail.

Law and Policies

The Director of National Intelligence (DNI) issued revised adjudicative guidelines (AG) in a Security Executive Agent Directive, effective on June 8, 2017. My ultimate decision would be the same under either set of adjudicative guidelines.

"[N]o one has a 'right' to a security clearance." Department of the Navy v. Egan, 484 U.S. 518, 528 (1988). 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." Id. at 527. The President has authorized the Secretary of Defense or his designee to grant applicants eligibility for access to classified information "only upon a finding that it is clearly consistent with the national interest to do so." Exec. Or. 10865 § 2.

[2] There is insufficient evidence of previous reports to human resources or that the security program manager was retaliating for past allegations against her.

[3] GE 2.

National security eligibility is predicated upon the applicant meeting the criteria contained in the adjudicative guidelines. These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, an administrative judge applies these guidelines in conjunction with an evaluation of the whole person. An administrative judge's overarching adjudicative goal is a fair, impartial, and commonsense decision. An administrative judge must consider a person's stability, trustworthiness, reliability, discretion, character, honesty, and judgment. AG ¶ 1(b).

The Government reposes a high degree of trust and confidence in persons with access to classified information. This relationship transcends normal duty hours and endures throughout off-duty hours. Decisions include, by necessity, consideration of the possible risk that the applicant may deliberately or inadvertently fail to safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation about potential, rather than actual, risk of compromise of classified information.

Clearance decisions must be made "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." Exec. Or. 10865 § 7. Thus, a decision to deny a security clearance 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.

Initially, the Government must establish, by substantial evidence, conditions in the personal or professional history of the applicant that may disqualify the applicant from being eligible for access to classified information. The Government has the burden of establishing controverted facts alleged in the SOR. See Egan, 484 U.S. at 531. "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). The guidelines presume a nexus or rational connection between proven conduct under any of the criteria listed therein and an applicant's security suitability. See ISCR Case No. 92-1106 at 3, 1993 WL 545051 at *3 (App. Bd. Oct. 7, 1993).

Once the Government establishes a disqualifying condition by substantial evidence, the burden shifts to the applicant to rebut, explain, extenuate, or mitigate the facts. Directive ¶ E3.1.15. An applicant has the burden of proving a mitigating condition, and the burden of disproving it never shifts to the Government. See ISCR Case No. 02-31154 at 5 (App. Bd. Sep. 22, 2005).

An applicant "has the ultimate burden of demonstrating that it is clearly consistent with the national interest to grant or continue his security clearance." ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002). "[S]ecurity clearance determinations should err, if they must, on the side of denials." Egan, 484 U.S. at 531; see AG ¶ 1(d).

Analysis

Guideline K: Handling Protected Information

AG ¶ 33 expresses the handling protected information security 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.

Relevant conditions that could raise a security concern under AG ¶ 34 and may be disqualifying include:

> (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;
>
> (g) any failure to comply with rules for the protection of classified or sensitive information; and
>
> (h) negligence or lax security practices that persist despite counseling by management.

Applicant's security violations are sufficient to implicate disqualifying security concerns under AG ¶¶ 34 (a), (g), and (h).

Relevant conditions that could mitigate security concerns under AG ¶ 35 include:

> (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;
>
> (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.

Applicant was employed with the same defense contractor from 1993 to 2015, completing his employment with that contractor as an information security specialist. He also has held a security clearance for more than 10 years. From 2012 to 2015, Applicant had four security incidents, resulting in verbal or written admonitions. There is sufficient evidence to support the SOR allegations, although the violations vary in individual seriousness. Taken together however, they indicate a carelessness or negligence with respect to protection of classified material. A pattern of violations is indicative of a problem with security awareness and a persistent lapse of expected conduct while working within a classified environment. These incidents raise concerns about Applicant's trustworthiness and good judgment. Applicant's testimony and evidence presented did little to diminish these concerns. The pattern of violations and the subsequent effort to hide the most recent incident lead me to question Applicant's future behavior with respect to security awareness and following rules and regulations for the safe handling of classified information. No mitigation is appropriate.

Guideline E; Personal Conduct

AG ¶ 15 expresses the personal conduct security concern:

> 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. Of special interest is any failure to cooperate or provide truthful and candid answers during national security investigative or adjudicative processes.

AG ¶ 16 describes conditions that could raise a security concern and may be disqualifying in this case. The following disqualifying condition are potentially applicable:

> (a) deliberate omission, concealment, or falsification of relevant facts from any personnel security questionnaire, personal history statement, or similar form used to conduct investigations, determine employment qualifications, award benefits or status, determine national security eligibility or trustworthiness, or award fiduciary responsibilities;
>
> (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;
>
> (c) credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any other single guideline, but which, when considered as a whole, supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, a lack of condor, unwillingness to comply with rules and regulations, or other

characteristics indicating that the individual may not properly safeguard classified or sensitive information; and

(e) personal conduct, or concealment of information about one's conduct, that creates a vulnerability to exploitation, manipulation, or duress by a foreign intelligence entity or other individual or group. Such conduct includes:

(1) engaging in activities which, if known, could affect the person's personal, professional, or community standing.

The allegations alleged under Guideline K that are cross-alleged under Guideline E (SOR ¶ 2.a) are specifically covered under Guideline K, and therefore AG ¶ 16(c) is not applicable. However, the conduct implicates AG ¶ 16(a), (b), and (e).

Applicant falsified his SCA and failed to voluntarily disclose the 2015 CAM to the Government investigator during his PSI. Applicant was clearly concerned about the potential consequences of reporting the 2015 incidents. He used great efforts to seek advice from coworkers and an authoritative opinion from his new employer's security manager as cover for not disclosing the information in his security clearance reapplication. However, Applicant did not fully inform his new security manager of all the facts related to the CAM, and failed to show sufficient evidence that the security manager provided an informed opinion and advice to omit the information from his SCA and PSI. Applicant's omission of the incidents that led to the 2015 CAM from his SCA and PSI was intentional and raises serious questions about his candor, judgment, and willingness to follow rules and regulations.

Guideline E includes conditions that could mitigate security concerns arising from personal conduct. I have considered all of the mitigating conditions under AG ¶ 17 and found the following relevant:

(a) the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts;

(b) the refusal or failure to cooperate, omission, or concealment was caused or significantly contributed to by advice of legal counsel or of a person with professional responsibilities for advising or instructing the individual specifically concerning security processes. Upon being made aware of the requirement to cooperate or provide the information, the individual cooperated fully and truthfully;

(c) 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; and

(d) 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 contributed to untrustworthy, unreliable, or other inappropriate behavior, and such behavior is unlikely to recur.

Applicant acknowledged three of four security lapses, but attempted to impugn the credibility of the security program manager who issued the CAM and hide its existence altogether with security investigators. Applicant did not fully inform his security manager of all the facts related to the CAM, and failed to show sufficient evidence that the security manager provided an informed opinion and advice to omit the information from his SCA and PSI. He intentionally failed to disclose the 2015 CAM in his SCA and did not voluntarily disclose the CAM during his PSI when confronted with an opportunity. I find that no mitigating condition fully applies.

Whole-Person Concept

Under AG ¶¶ 2(a), 2(c), and 2(d), the ultimate determination of whether to grant national security eligibility must be an overall commonsense judgment based upon careful consideration of the guidelines and the 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(d). Although adverse information concerning a single criterion may not be sufficient for an unfavorable eligibility determination, the individual may be found ineligible if available information reflects a recent or recurring pattern of questionable judgment, irresponsibility, or unstable behavior. AG ¶ 2(e).

I considered all of the potentially disqualifying and mitigating conditions in light of the facts and circumstances surrounding this case. I have incorporated my findings of fact and comments under Guidelines K and E in my whole-person analysis. Applicant is a mature employee with many years of handling classified information in sensitive spaces. The pattern of security lapses is indicative of a persistent problem that has not been shown to be rectified, and his intentional falsification of the SCA and PSI cement the concerns about his reliability and trustworthiness. The record evidence and consideration of the whole-person adjudicative factors are not sufficient to overcome the handling protected information and personal conduct concerns raised in the SOR.

Overall, the record evidence leaves me with questions and doubts as to Applicant's eligibility for continued access to classified information. Accordingly, I conclude Applicant has not carried his burden of showing that it is clearly consistent with the national security interests of the United States to continue his eligibility 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:	Against Applicant
Subparagraphs 1.a -1.d:	Against Applicant
Paragraph 2, Guideline E:	Against Applicant
Subparagraphs 2.a – 2.c:	Against Applicant

Conclusion

In light of all of the circumstances presented by the record in this case, it is not clearly consistent with the national interest to grant Applicant eligibility for a security clearance. Eligibility for access to classified information is denied.

_____
Gregg A. Cervi
Administrative Judge