DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 17-04374
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Mary M. Foreman, Esq., Department Counsel
For Applicant: *Pro se*

02/26/2019

_____

Decision

_____

CERVI, Gregg A., Administrative Judge

This case involves security concerns raised under Guidelines K (Handling Protected Information) and M (Use of Information Technology). Eligibility for access to classified information is granted.

Statement of the Case

Applicant submitted a security clearance application (SCA) on November 23, 2015. On February 12, 2018, the Department of Defense Consolidated Adjudications Facility (DOD CAF) sent him a Statement of Reasons (SOR) alleging security concerns under Guidelines K and M.[1]

Applicant responded to the SOR on March 11, 2018, and requested a hearing before an administrative judge. The case was assigned to me on June 18, 2018. The

[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) effective on June 8, 2017.

Defense Office of Hearings and Appeals issued a notice of hearing on August 1, 2018, and the hearing was convened on August 30, 2018. Government Exhibits (GE) 1 through 4 were admitted into evidence without objection. Applicant testified and Applicant Exhibits (AE) A through D were admitted without objection. DOHA received the hearing transcript (Tr.) on September 10, 2018.

Findings of Fact

Applicant is a 58-year-old system administrator, senior software engineer, and information systems security officer for a defense contractor, employed since 2008. Applicant married in 1980 and has two adult children. He received a bachelor's degree in 1991. He testified that he has held a DOD top secret security clearance for nearly 30 years.

The SOR alleges under Guideline K (Handling Protected Information), that Applicant committed security violations in 2015 by not properly securing classified information; and in 2016 by improperly using his system administrator logins and passwords, in violation of his privileged user agreement. The SOR also alleges that in 2017, his employer relieved him of his information system security officer and system administrator duties and access to system accounts following several inspection items from 2016 to 2017 that showed repeated failures to comply with system security requirements, policies, and procedures. The incidents described in SOR ¶¶ 1.b and 1.c were cross-alleged under Guideline M (Use of Information Technology). In his Answer to the SOR, Applicant admitted the two incidents in 2015 and 2016, but denied the 2017 allegation and the cross-allegation under Guideline M. The Government's evidence is sufficient to establish the SOR allegations.

SOR ¶ 1.a alleges Applicant failed to properly secure classified information. Applicant was appointed the information systems security officer (ISSO) by his employer in January 2015 after the previous ISSO retired. Applicant was not fully familiar with his duties and responsibilities, and relied on the security team supporting him, "on the job training," and the supervision of the information systems security manager (ISSM). Historical audit computer logs were backed up on rewritable compact discs (CD) that were marked with the appropriate security classification, since the information was being written from a classified system. The CDs were kept in plastic sleeves in a portfolio binder, marked with classification markings, and secured. Applicant's assistant ISSO (AISSO) was required to create the CDs for a historical record, until the company transferred all of the logs to external hard drives. The CDs were phased out, and another new AISSO was tasked to ensure the destruction of the old CDs. Applicant and his assistant emptied all of the CDs from their plastic sleeves in the binder, and sent the "empty" portfolio binder to a supply room to be reused. The supply room was in an access-controlled area, but not a classified controlled area. The binder was later discovered by an employee with one CD still in a sleeve. Applicant claims the CD did not have any classified information on it, but it was marked "classified" because the data came from a classified computer system. Applicant was cited for a security violation, but there was no evidence of loss, compromise

or suspected compromise of classified information found. Applicant took responsibility for the mistake, was given remedial training, and never repeated this security violation again.

SOR ¶ 1.b alleges Applicant improperly used his system administrator logins and passwords, and failed to follow user privileges and information assurance procedures. Shortly after assuming the ISSO position, Applicant was tasked to work on an information system (IS) with which he was previously unfamiliar. He was read into the program, and entered the particular lab in 2015, where he first saw a completely assembled IS system. He noted that the IS had not been certified, however it was already located in a special secured area. Applicant was tasked to certify it by the security official for the program. At the time, common practice was to allow the ISSO to log into the system using root credentials, but that practice was later stopped. Applicant met with the security staff for the program and explained what he needed to do to certify the IS, and Applicant requested that the security department permit another system administrator (SA) who developed the IS, to assist him. The SA was briefed by the program security officer and permitted to enter the space. Applicant later learned that the security official was not authorized to give the SA both a general user and a privileged user briefing at once. One of the briefings should have been done by another security office within the company, but Applicant noted it was often done by the same person. According to Applicant, once the oversight was discovered, the SA received the proper authorization "within five minutes," and believed his actions were authorized and the most efficient method to accomplish the task.

Applicant was also alleged to have continued to use the root account for logins after the system had been certified, and that he failed to document the logins using the root account for tracking and auditing purposes. Applicant explained that using the root credentials was the only way to solve the problems with the IS, and that the security department should have made logs available to be used to document occasions where the root certification was used. However, Applicant took responsibility for not logging the uses properly, and testified that logins were in fact traceable, even without the logs. As a result of the security violation, Applicant was denied access to particular programs operated by that military branch. No evidence of loss, compromise, or suspected compromise of classified information was found.

SOR ¶ 1.c alleges that Applicant was relieved of his ISSO duties and access to secure areas in October 2017, after self-inspections disclosed repeated failures to comply with the information system configuration and operational security requirements, policies, and procedures. In particular, the Government's evidence shows various non-compliance issues with users on the system, user briefings, seal logs, incomplete permissions and auditing settings, poor maintenance log retention, laptop CD/DVD drive and removable media controls not configured properly, and no system warning banner displayed. In addition, Applicant did not correct the deficiencies within the two-week period provided.

Applicant explained that he was responsible for keeping track of 200 user authorizations for 18 systems. There were discussions and changes to the user authorization procedures and forms during this period, and that the system in question

was housed at a military base under a mobile deployment plan to allow it to be operated in the field. At the same time the system was returned to Applicant's facility for audits, patching, and updates after a longer-than-usual period outside the facility, a self-inspection was conducted. Applicant supported the self-inspection and was interested in seeing the results so that he could make the corrections and return the system back to the field. Applicant argued that the ISSM agreed with the field engineers to permit them to create user accounts and were responsible for the system while it was outside Applicant's facility. Applicant did not have physical access to the system or oversight while it was in the field, and the engineers improperly created new user accounts for personnel that needed access while the system was deployed.

Applicant sent his ASSOs to the meeting to discuss the self-inspection findings because of a conflict, and later learned that his ASSOs did not make the simple corrections to fix the deficiencies. Applicant's access was denied before he could inspect the system on his own, and was not fully apprised of the deficiencies after the self-inspection. After being denied access, Applicant spent the next two weeks instructing his ASSOs on how to correct the deficiencies. Applicant admits he should have been more forceful in demanding the list of findings of the self-inspection and more proactive in addressing the problems, but relied on others to do the work. Applicant agrees that he was responsible for supervising his ASSOs in completing the work required, but notes that security rules changed after the system was certified for deployment. He disagreed with some of the findings regarding hard drives, and asserted that the ISSM shared responsibility for the system, certified it for mobile deployment, and should have worked with him to correct deficiencies once they were discovered, rather than deny him access. He also acknowledged that he was aware of one previous user agreement deficiency before the 2017 findings, but not the other previous deficiencies noted in the self-inspection report. No compromise of classified information or counter-intelligence implications were found as a result of the incidents discussed above.

Applicant emphatically denies any intention to violate security rules or procedures during any of the incidents listed in the SOR. He had never had a security violation in the past, despite nearly 30 years with a top secret security clearance. He believes the large volume of work and poor training and directions from his manager led to the eventual security violations. Applicant submitted a detailed narrative response to the allegations, a 2016 security training certification, a certificate of recognition from his company, and other documents in support of his testimony. His testimony was comprehensive, straightforward, and sincere, while always maintaining his professionalism.

Applicant's former information systems security risk manager and former ISSM at the company provided a signed, sworn statement of support for Applicant, and claimed that three unnamed employees within the information security office targeted Applicant and other employees to interpret the rules to find security infractions in order to cause them to lose their security clearance and job. He noted that once an infraction was found, the employee had very little recourse in defense. He also noted that Applicant was trustworthy, and called him an asset to the community that cares about protecting classified information and a proud supporter of the warfighter. No corroborating evidence

of inappropriate behavior of security personnel at the company was presented at the hearing, but Applicant quoted the writer's claim in his Answer to the SOR.

Another coworker attested to Applicant's good judgment, stating he would never knowingly violate security regulations or procedures, and noted Applicant was conscientious, stable, caring, and trustworthy. A director of security for another defense contractor who has known Applicant since 1987 when they were friends and coworkers, wrote of Applicant's "great integrity." A current engineer at Applicant's company wrote of Applicant's reliability, good judgment, stability, and responsibility. He notes situations where Applicant steadfastly followed security rules to maintain security compliance regardless of user complaints or inconvenience.

Policies

"[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.

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. *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, e.g.,* ISCR Case No. 12-01295 at 3 (App. Bd. Jan. 20, 2015).

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, e.g.,* 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:

> (b) collecting or storing protected information in any unauthorized location;
>
> (c) loading, drafting, editing, 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 sensitive information; and
>
> (h) negligence or lax security practices that persist despite counseling by management.

The evidence presented is sufficient to raise the security concerns described above.

Guideline K includes conditions that could mitigate security concerns arising from incidents regarding handling protected information. 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.

The security violations from 2015 to 2017 described in the SOR were adequately addressed and in some cases, plausibly contested by Applicant. He has held a security clearance for nearly 30 years without incident before these incidents occurred. There is some evidence that he was appointed ISSO without sufficient training or direction. He acknowledged the 2015 and 2016 incidents, and took responsibility for not adequately supervising his assistants in response to the 2017 self-inspection report. He noted that he should have been more proactive and aggressive in ensuring he understood the deficiencies and addressed them in a timely manner. However, Applicant generally denies responsibility for the 2017 deficiencies found on a system that was outside his control for an extended period of time, and operated under an agreement between his manager and the company engineers.

Regardless of the actual security violations imputed to Applicant by reason of his direct action or supervisory responsibilities, the evidence does not suggest a pattern of rules violations outside of isolated incidents. There was no compromise of classified information, and the counter-intelligence review did not reveal a concern. There is adequate evidence to suggest that Applicant attempted to perform his duties as assigned, but the direction and training were insufficient to prevent the security incidents from occurring. Disputes over subject matter knowledge or work performance do not necessarily implicate security concerns. Applicant did not hide any incidents, and accepted responsibility for his role and willingly participated in retraining when offered. Based on his limited experience as an ISSO, he is now more attuned to the potential pitfalls while performing similar tasks. Applicant is strongly supported by his former ISSM

and co-workers who attest to his trustworthiness and security consciences. AG ¶¶ 35(a), (b), (c), and (d) apply.

Guideline M: Use of Information Technology Systems

AG ¶ 39 expresses the security concern pertaining to use of information technology systems:

> Failure to comply 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.

Relevant conditions that could raise a security concern under AG ¶ 40 and may be disqualifying include:

> (g) negligence or lax security practices in handling information technology that persists despite counseling by management.

The evidence presented is minimally sufficient to raise the security concern described above, and a similar security concern is included under AG ¶ 34 (Guideline K). The findings of fact, discussion, reasoning, and mitigation applicable under Guideline K, apply equally to the concern raised under Guideline M, and are incorporated herein. Therefore, no additional discussion of Guideline M concerns is required.

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).

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 M, in my whole-person analysis. I also considered Applicant's long history of employment and security eligibility. I am convinced that the security incidents identified in the SOR were unintentional, isolated incidents. No compromise of classified information was found. Based on the testimony and documentary evidence, I am convinced that these incident are behind him and similar violations are unlikely to recur. I have no doubts about Applicant's judgment, honesty, and trustworthiness.

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 - 1.c:	For Applicant
Paragraph 2, Guideline M:	FOR APPLICANT
Subparagraph 2.a:	For Applicant

Conclusion

I conclude that it is clearly consistent with the national security interests of the United States to continue Applicant's eligibility for access to classified information. Applicant's security clearance is granted.

_____
Gregg A. Cervi
Administrative Judge