DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
[Redacted]	)	ISCR Case No. 11-12684
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Eric H. Borgstrom, Esq., Department Counsel
For Applicant: *Pro se*

02/28/2014

Decision

FOREMAN, LeRoy F., Administrative Judge:

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

Statement of the Case

On August 27, 2013, the Department of Defense (DOD) sent Applicant a Statement of Reasons (SOR) alleging security concerns under Guidelines K and E. DOD acted under Executive Order 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 DOD on September 1, 2006.

Applicant received the SOR on September 9, 2013; answered it on September 27, 2013; and requested a hearing before an administrative judge. Department Counsel was ready to proceed on December 23, 2013, and the case was assigned to me on January 3, 2014. The Defense Office of Hearings and Appeals (DOHA) issued a notice

of hearing on January 6, 2014, scheduling the hearing for January 14, 2014. On January 9, 2014, DOHA issued an amended notice of hearing, rescheduling the hearing for January 15, 2014. I convened the hearing as rescheduled. Applicant affirmatively waived the 15-day notice requirement of the Directive ¶ E3.1.8. (Hearing Exhibit (HX) I.) Government Exhibits (GX) 1 through 11 were admitted in evidence without objection. Applicant testified but did not present any documentary evidence or the testimony of any other witnesses. I kept the record open until January 31, 2014, to enable Applicant to submit documentary evidence. He timely submitted AX A through F, which were admitted without objection. Department Counsel's comments regarding AX A through F are attached to the record as HX II. At my request, Department Counsel also presented extracts of the manuals cited in the SOR, and they are attached to the record as HX III. DOHA received the transcript (Tr.) on January 30, 2014.

Amendment of SOR

The SOR ¶ 2.a alleged that Applicant was debriefed from all classified access and resigned in lieu of involuntary termination because of the conduct alleged in SOR ¶¶ 1.a, 1.b, and 1.c. However, there is no SOR ¶ 1.c. I granted Department Counsel's motion to amend the SOR to allege that Applicant's debriefing and resignation were because of the conduct alleged in SOR ¶¶ 1.a and 1.b. (Tr. 57.)

Findings of Fact

In his answer to the SOR, Applicant admitted all the allegations in the SOR. His admissions in his answer and at the hearing are incorporated in my findings of fact.

Applicant is a 65-year-old senior systems architect employed by a defense contractor. He served in the U.S. Marine Corps from January 1969 to December 1972. He held a security clearance while in the Marine Corps. (Tr. 30.) He received a bachelor's degree in June 1976 and a master's degree in June 1981. He was employed as a software engineer in the private sector from November 1985 to March 1998. He was employed by defense contractors from March 1998 to January 2011, when he resigned in lieu of termination. He began working for his current employer in February 2011. He has held a security clearance since March 1998.

On August 20, 2010, Applicant was preparing an unclassified summary of a cryptographic key management plan. He was working alone and no one checked his work. He inadvertently used a classified acronym in the summary. The acronym indicates what kind of cryptography was being used, but it did not reveal any cryptographic keys. (Tr. 16.) Using unclassified but encrypted email, he sent the summary to another contractor location for review by several employees. A recipient notified him that use of the acronym was a potential spill of classified data and notified the security office of the potential spill. Applicant was counseled on his responsibilities and briefed on the appropriate use of security classification guidance. (GX 5; Tr. 36-38.)

Applicant saved the summary under a new file name, and he inadvertently also saved it under its old name, thus creating two contaminated files. The error was discovered when he emailed the contaminated file under the old name to a fellow employee. His supervisors discovered this error on August 25, 2010. Applicant was required to complete additional training on the use of classified information and prevention of data spills, and he received a written reprimand. (GX 6.)

Investigation of the spill revealed that the classified document had been placed on a shared directory as early as October 5, 2010, and it was placed on a shared network on December 16, 2010. (GX 7.) On January 3, 2011, the contaminated summary was attached to an unclassified meeting notice emailed to 11 cleared employees.

During the investigation of the data spill, Applicant was interviewed by his supervisor and facility security officer (FSO), and they concluded that he was not fully forthcoming during the interviews. (GX 9.) The FSO's final report stated that Applicant "reported contradictory information and did not immediately disclose all information concerning the location of the contaminated file." (GX 10 at 2.)

All three spillage incidents were characterized as infractions rather than violations on the security incident reports. (GX 5, 6, and 9.) Based on Applicant's perceived lack of candor and three security infractions during a six-month period, he was debriefed from all classified programs on January 6, 2011.[1] On the same day, he resigned. (GX 9.) At the hearing, he testified that he was told that resignation was "advisable," and he assumed that he would be involuntarily terminated if he did not resign. (Tr. 46.)

At the hearing, Applicant denied intentionally providing contradictory information to his supervisor and FSO. He testified that the spreadsheet did not yet exist when he first distributed the contaminated summary. He added the summary to the spreadsheet later, and he believed that he cut and pasted the summary into the spreadsheet without checking it for classified data. (Tr. 47-48.) He testified that when he was questioned by his supervisor and the FSO, that he did not realize that the contaminated summary had been copied onto the spreadsheet and distributed with the meeting notice. (Tr. 50.)

Applicant had no security violations from 1998 until the incidents in the SOR. (Tr. 46.) He understands the inherent danger of trying to discuss classified information in an unclassified document. He testified that he has learned his lesson from his security infractions and he has become more reliable because he is aware of the "subtle pitfalls" in the classified information system. (Tr. 20-22.)

Three long-time friends and professional associates submitted letters on Applicant's behalf, describing him as honest, skilled, and committed to his work. (AX A

[1] There is no evidence in the record indicating that Applicant's clearance was revoked. At the hearing, he stated that he was seeking to "retain" his security clearance. (Tr. 13.)

[two statements]; AX C.) Three colleagues at his current place of employment submitted statements attesting to his technical knowledge, leadership, integrity, and responsibility. (AX D; AX E; AX F.) His performance appraisals for the last two years have been outstanding, and he has received two pay raises since being hired. (AX B.)

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, *Safeguarding Classified Information within Industry* § 2 (Feb. 20, 1960), as amended.

Eligibility for a security clearance is predicated upon the applicant meeting the criteria contained in the AG. 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 all available and reliable information about the person, past and present, favorable and unfavorable.

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." *See* 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 ¶ 2(b).

Analysis

Guideline K, Handling Protected Information

The SOR alleges that in August 2010, Applicant improperly emailed a file containing classified information via an unclassified network (SOR ¶ 1.a), and that on or about January 3, 2011, he emailed a classified file, improperly marked unclassified, that compromised classified information (SOR ¶ 1.b). The security concern under this guideline 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 concern."

Security violations are one of the strongest possible reasons for denying or revoking access to classified information, as they raise very serious questions about an applicant's suitability for access to classified information. Once it is established that an applicant has committed a security violation, he or she has a very heavy burden of demonstrating that he or she should be entrusted with classified information. Because security violations strike at the very heart of the industrial security program, an administrative judge must give any claims of reform and rehabilitation strict scrutiny. *See* ISCR Case No. 03-26888 (App. Bd. Oct. 5, 2006).The frequency and duration of the security violations are aggravating factors. ISCR Case No. 97-0435 at 5 (App. Bd. July 14, 1998).

The SOR alleges that Applicant violated Department of Defense 5220.22M, *National Industrial Security Program Operating Manual (NISPOM),* as amended, paragraphs 4-200, 4-210b, and 5-100. Paragraph 4-200 requires classified information to bear appropriate markings to warn and inform holders of the information of the degree of protection required. Paragraph 4-210b requires that electronically transmitted messages be marked in the same manner as other documents, with certain exceptions not applicable to this case. Paragraph 5-11 makes contractors responsible for

safeguarding classified information in their custody or under their control, and it makes individuals responsible for classified information entrusted to them.

The evidence establishes the following disqualifying conditions under this guideline:

> AG ¶ 34(c): loading, drafting, editing, modifying, storing, transmitting, or otherwise handling classified reports, data, or other information on any unapproved equipment . . . ;
>
> AG ¶ 34(g): any failure to comply with rules for the protection of classified or other sensitive information; and
>
> AG ¶ 34(h): negligence or lax security habits that persist despite counseling by management.

The following mitigating conditions are potentially relevant:

> 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; and
>
> 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.

AG ¶ 35(a) is established. Applicant's security infractions occurred more than three years ago. They arose from a single instance of using a classified acronym in a document, but another infraction occurred when Applicant inserted the same contaminated document into a meeting notice without ensuring that it had been sanitized. Applicant's infractions in August 2010 and January 2011 occurred after he had held a security clearance for 12 years, apparently without incident. He has gained a good reputation for attention to detail, honesty, integrity, and responsibility since finding new employment in February 2011.

AG ¶ 35(b) is partly established. Applicant did not respond favorably to his remedial training and reprimand in August 2010, because his inattention caused the infraction in January 2011. However, since his change of jobs in February 2011, he has demonstrated his reliability and attention to detail. At the hearing, he testified that he has learned from his experience and is more aware of the "subtle pitfalls" of working with classified information.

Guideline E, Personal Conduct

The SOR alleges that, as a result of the conduct alleged under Guideline K, Applicant was debriefed from all classified access and resigned in lieu of involuntary termination. Although Applicant's resignation in lieu of termination was based in part on the conclusions of his supervisor and FSO that he was not entirely candid during the investigation of his security infractions, his lack of candor was not alleged in the SOR.

The concern under this guideline is set out in AG ¶ 15 as follows:

> 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.

Applicant's security infractions are sufficient to establish the following disqualifying conditions under this guideline:

> AG ¶ 16(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, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the person may not properly safeguard protected information; and
>
> AG ¶ 16(d): 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 . . . a pattern of dishonesty or rule violations.

The following mitigating conditions are potentially relevant:

> AG ¶ 17(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

> AG ¶ 17(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 caused untrustworthy, unreliable, or other inappropriate behavior, and such behavior is unlikely to recur.

AG ¶ 17(c) is established. Although Applicant's former employer characterized his inadvertent use of a classified acronym as an "infraction" rather than a "violation," I am not convinced that the data spill was "minor" within the meaning of this guideline. However, the data spill was limited to a small group of individuals holding security clearances and each infraction occurred during a relatively short time period. Applicant held a security clearance for 12 years without incident before committing the infractions. He has learned from his experience and is committed to being more vigilant regarding the "subtle pitfalls" that can occur when handling classified information.

AG ¶ 17(d) is established. Applicant did not receive "counseling" in the traditional sense, but he received remedial training and was reprimanded. He apparently did not benefit from these measures at first, because he committed the second infraction shortly thereafter. However, his loss of employment appears to have captured his attention and he is committed to meticulous compliance with rules and procedures for handling classified information.

Whole-Person Concept

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. In applying the whole-person concept, an 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. An 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.

I have incorporated my comments under Guidelines K and E in my whole-person analysis. Some of the factors in AG ¶ 2(a) were addressed under those guidelines, but some warrant additional comment.

Because the SOR did not allege any lack of candor during the investigation of his infractions, it cannot be an independent basis for denying him access to classified information. However, conduct not alleged in the SOR may be considered to assess an applicant's credibility; to decide whether a particular adjudicative guideline is applicable; to evaluate evidence of extenuation, mitigation, or changed circumstances; to consider whether an applicant has demonstrated successful rehabilitation; or as part of a whole-person analysis. ISCR Case No. 03-20327 at 4 (App. Bd. Oct. 26, 2006). I have considered Applicant's responses to questioning by his supervisor and FSO during the investigation of his infractions for these limited purposes. Based on all the evidence, including my observation of Applicant's demeanor during the hearing, I am satisfied that he was not being evasive or untruthful during that investigation. His failure to fully describe all the locations where the contaminated document was filed was due to his own negligent failure to track down the locations where he filed it. It was not due to intentional evasion, falsification, or an effort to minimize his culpability.

Applicant was candid, sincere, and credible at the hearing. He served honorably in the U.S. Marine Corps and held a clearance during his military service. He has held a security clearance and worked on sensitive projects related to national defense since 1998. He has rebounded from his resignation in lieu of termination and established a reputation for honesty, integrity, and reliability since finding new employment in February 2011.

After weighing the disqualifying and mitigating conditions under Guidelines K and E, evaluating all the evidence in the context of the whole person, and mindful of my obligation to resolve close cases in favor of national security. I conclude Applicant has mitigated the security concerns based on his handling of protected information and personal conduct. Accordingly, I conclude he has carried his burden of showing that it is clearly consistent with the national interest to continue his eligibility for access to classified information.

Formal Findings

I make the following formal findings on the allegations in the SOR:

Paragraph 1, Guideline K (Handling Protected Information):	FOR APPLICANT
Subparagraphs 1.a-1.b:	For Applicant
Paragraph 2, Guideline E (Personal Conduct):	FOR APPLICANT
Subparagraph 2.a:	For Applicant

Conclusion

I conclude that it is clearly consistent with the national interest to grant Applicant eligibility for a security clearance. Eligibility for access to classified information is granted.

LeRoy F. Foreman
Administrative Judge