DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
----------	)	ISCR Case No. 11-06831
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Candace Garcia, Esq., Department Counsel
For Applicant: Kelly W. McNulty, Esq.

05/17/2012

Decision

LEONARD, Michael H., Administrative Judge:

Applicant contests the Defense Department's intent to revoke his eligibility for a security clearance. The evidence shows Applicant was negligent or lax in his duties as the facility security officer (FSO) of a small company that provides alarm monitoring services to defense contractors. In 2010 the Defense Security Service (DSS) issued a culpability report citing Applicant for disregarding security requirements and attempting to mislead the DSS during a formal inquiry. The major deficiency was corrected by obtaining security clearances for all employees who monitor alarms, and the alarm company has been in compliance with security requirements since November 2010. The evidence is not sufficient to establish that Applicant made deliberately false or misleading statements during the inquiry. Accordingly, this case is decided for Applicant.

Statement of the Case

Acting under the relevant Executive Order and DoD Directive,[1] on or about November 9, 2011, the Defense Office of Hearings and Appeals (DOHA) sent Applicant a statement of reasons (SOR), explaining it was unable to find that it was clearly consistent with the national interest to grant Applicant access to classified information. The SOR is similar to a complaint, and it detailed the reasons for the action under the security guidelines known as Guideline K for handling protected information and Guideline E for personal conduct.

Applicant timely answered the SOR and requested a hearing. The hearing took place April 10, 2012. The transcript (Tr.) was received April 16, 2012.

Rulings on Procedure

As requested, I took administrative or official notice of the following provisions of the NISPOM:[2]

> ¶ 3-102. Contractors shall be responsible for ensuring that the FSO, and others performing security duties, complete security training considered appropriate by the CSA. Training requirements shall be based on the facility's involvement with classified information and may include an FSO orientation course and for FSOs at facilities with safeguard capability, an FSO Program Management Course. Training, if required, should be completed within 1 year of appointment to the position of FSO.
>
> ¶ 5-900. This section [referring to Section 9 on Intrusion Detection Systems (IDS)] specifies the minimum standards for an approved IDS when supplemental protection is required for TOP SECRET and SECRET material. The IDS shall be connected to, and monitored by, a central monitoring station. Alarm system installation shall conform to the requirements of this section or to the standards set forth in reference (o). The CSA will approve contingency protection procedures in the event of IDS malfunction.

---

[1] This case is adjudicated under Executive Order 10865, *Safeguarding Classified Information within Industry*, signed by President Eisenhower on February 20, 1960, as amended, as well as DoD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program*, dated January 2, 1992, as amended (Directive). In addition, the *Adjudicative Guidelines for Determining Eligibility for Access to Classified Information* (AG), effective within the Defense Department on September 1, 2006, apply here. The AG were published in the Federal Register and codified in 32 C.F.R. § 154, Appendix H (2006). The AG replace the guidelines in Enclosure 2 to the Directive.

[2] All references to the NISPOM refer to the February 2006 edition of the National Industrial Security Program Operating Manual, which is a Defense Department publication known as DoD 5220.22-M. The NISPOM is a set of standards and guidelines for securing classified material, information, and equipment to be developed, stored, or maintained by a government contractor.

¶ 5-902.b. SECRET-cleared central station employees shall be in attendance at the alarm monitoring station in sufficient number to monitor each alarmed area within the cleared contractor facility.[3]

Findings of Fact

The SOR alleged essentially three items: (1) under Guideline K, Applicant violated ¶ 5-902.b of the NISPOM by permitting uncleared personnel to monitor alarms of cleared defense contractor facilities; (2) under Guideline K, Applicant violated ¶ 3-102 of the NISPOM by failing to complete FSO training; and (3) under Guideline E, Applicant made misleading statements "and/or" conflicting statements about his duties "and/or" the established procedures for alarm monitoring of cleared facilities.[4] In addition to those three items, the SOR cross referenced the Guideline K allegations under Guideline E. He denied the allegations in his answer to the SOR. The following findings of fact are supported by substantial evidence.

Applicant is a 46-year-old customer service manager and FSO for a small company of less than 100 employees. The company provides alarm monitoring services to a variety of customers, to include defense contractors. Although the alarm company has never had classified information on its premises, it is required to have a facility clearance to provide alarm monitoring services to companies that do.

Applicant has been continuously employed by the alarm company for more than 20 years. His education background includes a bachelor's degree. He is seeking to retain a security clearance that was previously granted to him in 2004.[5] In this regard, he has the support of the company president and owner, who appeared as a witness at the hearing. The company president believes that Applicant is a trustworthy employee.[6]

Applicant has served as the FSO since 2004, which is when the alarm company first applied for a facility clearance to provide services to a certain customer.[7] A few months after the initial application, the DSS, which is an agency of the Defense

---

[3] Appellate Exhibits I and II.

[4] The SOR allegations are not a model of clarity. For example, using the phrase "*and/or* has been vilified for most of its life–and rightly so. The upshot is that 'the only safe rule to follow is not to use the expression in any legal writing, document or proceeding, under any circumstances.'" *A Dictionary of Modern Legal Usage* 56 (Bryan A. Garner ed., 2nd ed., 1995) (internal citation omitted). A longstanding and still leading authority on the requirements of the plain English style has described *and/or* as "[a] device, or shortcut, that damages a sentence and often leads to confusion and ambiguity." William Strunk Jr. & E.B. White, *The Elements of Style* 40, 4th ed. 1999. As noted above, I have attempted to state the gravamen of the SOR allegations. The findings of fact should help flesh out the relevant details.

[5] Exhibits 1 and 2.

[6] Tr. 155.

[7] Exhibit A at 2–5.

Department that serves as an interface between the government and the defense industry, granted the alarm company a facility clearance at the interim secret level.[8] By September 2004, the DSS had completed its initial review of the company and determined the alarm company was in compliance with a satisfactory rating.[9] And by January 2005, the DSS had completed its work and granted the alarm company a facility clearance at the secret level.[10]

The alarm company held the facility clearance without incident until the fall of 2006, when the facility clearance was administratively terminated due to a lack of a bona fide requirement for classified services.[11] The administrative termination was not a negative reflection on the alarm company. Within the allowed two-year-period, the alarm company's facility clearance was reprocessed in late 2007 or early 2008 based on a request from a defense contractor, Company 1, which anticipated the need for employees of the alarm company to have security clearances.[12]

In November 2009, the DSS completed a review of the alarm company and determined it was in general compliance with a satisfactory rating.[13] Although the review was favorable, it also made several administrative findings, which are items that required attention and corrective action. The administrative findings included Applicant had not completed FSO training, had not obtained a JPAS account, and did not have access to the NISPOM, matters he was told to complete by the DSS during initial processing of the facility clearance in 2007–2008.[14] The alarm company, through Applicant as FSO, replied to the administrative findings with corrective actions in early 2010, to include Applicant's completion of FSO training. Through the November 2009 review, the DSS, via three different industrial security representatives (IS Rep) that had conducted reviews, had not expressed a concern about how the alarm company was monitoring its alarms.[15] At the time, the only two cleared employees of the alarm company were Applicant, as the FSO, and the company president.

That situation changed in about June 2010, when the IS Rep learned that the alarm company was not using cleared employees to monitor the alarms of cleared

[8] Exhibit A at 6.

[9] Exhibit A at 12.

[10] Exhibit A at 13.

[11] Exhibit A at 14-15.

[12] Exhibit A at 16-17; Tr. 47-48.

[13] Exhibit A at 18.

[14] Exhibit 4 at 4.

[15] Tr. 51-52.

defense contractors as required by ¶ 5-902.b of the NISPOM.[16] The alarm company was then monitoring the alarms for three defense contractors: (1) Company 1, which had a facility clearance at the secret level;[17] (2) Company 2, which had a facility clearance at the confidential level;[18] and (3) Company 3, which was not a cleared company.[19] The IS Rep made this discovery when he intentionally tripped an alarm at a Company 2 facility. The alarm signal was detected by the alarm company, and alarm monitors followed their normal procedures of notifying Company 2 security when their requests for the password were not answered. On the day in question, Applicant and the company president were not present in the alarm monitoring station because Applicant was out-of-state on vacation and the company president was piloting an aircraft on other business. As a result, none of the alarms of the three companies, including the alarms of Company 1, which was cleared at the secret level, were being monitored by cleared employees in attendance at the alarm monitoring station.

According to the administrative inquiry, the IS Rep concluded that the processes and procedures of the alarm company were appropriate except for the lack of security clearances for the employees who monitor the alarms.[20] The IS Rep also interviewed Applicant as part of the inquiry. According to that document (the IS Rep did not appear as a witness at the hearing), Applicant:

> [M]odified his responses depending on the question asked and the chronology of events during the inquiry. At the beginning of the inquiry he said he monitored all of the UL 2050 alarms. Later he said he gets notified of the alarm and he performed all of the required actions. Later still he said the Alarm Room Supervisor could override the system and handle the alarm and notification. Finally he admitted that the alarm monitors had the same access to the UL 2050 alarms as they had to the other alarms they monitored (commercial burglary alarms).[21]

---

[16] Exhibit 4. The exhibit consists of a one-page culpability report and a three-page administrative inquiry, which is an attachment to the report.

[17] Exhibit A at 64-65. This is the same Company 1 mentioned in paragraph five of the findings.

[18] Exhibit A at 66-67.

[19] Exhibit 4 at 2.

[20] Exhibit 4 at 2-3.

[21] Exhibit 4 at 3. UL 2050 refers to an independent organization called Underwriters Laboratories (UL), which developed a set of standards that would meet and often surpass the standards in the NISPOM. These standards are known as UL 2050 in the defense industry. The alarm company president had a role in the UL 2050 process. Tr. at 39-40.

The IS Rep concluded that there was no compromise of classified information, and the likelihood of unauthorized access was "very remote."[22] Based on the inquiry, the DSS issued a culpability report, which concluded that Applicant "appears culpable of knowingly disregarding NISPOM requirements and attempting to mislead" the IS Rep during the formal inquiry.[23]

Over the next several months, Applicant, with the concurrence of the company president, worked with the IS Rep to implement the recommendation of the administrative inquiry to obtain security clearances for enough employees to comply with the NISPOM.[24] Applicant and the company decided to have all alarm monitors obtain security clearances to avoid scheduling problems, and approximately 21 employees were granted security clearances. This corrective action was successfully completed on November 4, 2010, when the DSS determined the alarm company was in compliance with the NISPOM.[25] The alarm company's status was reaffirmed in October 2011, when the same IS Rep inspected the alarm company and determined it was in compliance with a security posture of satisfactory.[26] Currently, each shift of alarm monitors consists of employees who have security clearances at the secret level.[27]

Law and Policies

It is well-established law that no one has a right to a security clearance.[28] As noted by the Supreme Court in *Department of Navy v. Egan*, "the clearly consistent standard indicates that security clearance determinations should err, if they must, on the side of denials."[29] Under *Egan,* Executive Order 10865, and the Directive, any doubt about whether an applicant should be allowed access to classified information will be resolved in favor of protecting national security.

---

[22] Exhibit 4 at 3.

[23] Exhibit 4 at 1.

[24] Exhibit A at 36-41.

[25] Exhibit A at 63.

[26] Exhibit A at 82.

[27] Tr. 78-79.

[28] *Department of Navy v. Egan*, 484 U.S. 518, 528 (1988) ("it should be obvious that no one has a 'right' to a security clearance"); *Duane v. Department of Defense*, 275 F.3d 988, 994 (10th Cir. 2002) (no right to a security clearance).

[29] 484 U.S. at 531.

A favorable clearance decision establishes eligibility of an applicant to be granted a security clearance for access to confidential, secret, or top-secret information.[30] An unfavorable decision (1) denies any application, (2) revokes any existing security clearance, and (3) prevents access to classified information at any level.[31]

There is no presumption in favor of granting, renewing, or continuing eligibility for access to classified information.[32] The Government has the burden of presenting evidence to establish facts alleged in the SOR that have been controverted.[33] An applicant is responsible for presenting evidence to refute, explain, extenuate, or mitigate facts that have been admitted or proven.[34] In addition, an applicant has the ultimate burden of persuasion to obtain a favorable clearance decision.[35] In *Egan*, the Supreme Court stated that the burden of proof is less than a preponderance of the evidence.[36] The DOHA Appeal Board has followed the Court's reasoning, and a judge's findings of fact are reviewed under the substantial-evidence standard.[37]

The AG set forth the relevant standards to consider when evaluating a person's security clearance eligibility, including disqualifying conditions and mitigating conditions for each guideline. In addition, each clearance decision must be a commonsense decision based upon consideration of the relevant and material information, the pertinent criteria and adjudication factors, and the whole-person concept.

The Government must be able to have a high degree of trust and confidence in those persons to whom it grants access to classified information. The decision to deny a person a security clearance is not a determination of an applicant's loyalty.[38] Instead, it is a determination that an applicant has not met the strict guidelines the President has established for granting eligibility for access.

---

[30] Directive, ¶ 3.2.

[31] Directive, ¶ 3.2.

[32] ISCR Case No. 02-18663 (App. Bd. Mar. 23, 2004).

[33] Directive, Enclosure 3, ¶ E3.1.14.

[34] Directive, Enclosure 3, ¶ E3.1.15.

[35] Directive, Enclosure 3, ¶ E3.1.15.

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

[37] ISCR Case No. 01-20700 (App. Bd. Dec. 19, 2002) (citations omitted).

[38] Executive Order 10865, § 7.

Discussion

1. Handling Protected Information

The security concern under Guideline K for handling protected information is:

> 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.[39]

The guideline has several conditions that could raise security concerns and may be disqualifying.[40] The following conditions are most pertinent:

> 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.

Concerning SOR ¶ 1.a, the parties skirmished on the question if Company 2 was cleared at the secret or confidential level, as that related to the applicability of ¶ 5-902.b of the NISPOM when read in light of ¶ 5-900 of the NISPOM. In the findings of fact, I found Company 2 was cleared at the confidential level based on specific documentary evidence presented by Applicant as opposed to general documentary evidence presented by the Government. Nevertheless, the question is a bit off point because the allegation was not limited to Company 2. The allegation is broad enough to include Company 1 based on the following plain language in SOR ¶ 1.a: "permitted uncleared personnel to monitor the alarms of cleared contractor facilities." The evidence as a whole shows the alarm company, and therefore Applicant as the FSO, failed to comply with ¶ 5-902.b by allowing uncleared employees to monitor the alarms of Company 1, which was cleared at the secret level. The fact that the matter came to light during an inspection of a Company 2 facility, which was cleared at the confidential level, is largely beside the point.

Concerning SOR ¶ 1.b, Applicant, as the FSO of the alarm company, did not act with sufficient promptness and took too long to complete FSO training. In doing so, he was in violation of ¶ 3-102 of the NISPOM. Likewise, although not alleged as a violation of the NISPOM, he was negligent or lax in not obtaining a JPAS account and not having access to the NISPOM when told to complete those tasks by the IS Rep in 2009.

---

[39] AG ¶ 33.

[40] AG ¶ 34(a)–(i).

The guideline also has three conditions that could mitigate security concerns.[41] Although all three may have some applicability, the following is most pertinent:

> 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.

For reasons not entirely clear from the record, the alarm company was allowed to operate with a facility clearance without a sufficient number of cleared employees to monitor the alarms of cleared defense contractors. The DSS, knowingly or unknowingly, permitted this practice for some period. After the 2010 incident, Applicant, with the support of the company president, took the corrective action of obtaining security clearances for all employees who monitor alarms. That action was completed within a matter of months, the alarm company was back in compliance by November 2010, and it has remained in compliance to date. A recurrence of similar conduct is unlikely because the corrective action nearly guarantees the alarms will be monitored by cleared employees. The other security matters, such as the FSO training, were addressed by corrective actions before the 2010 incident and they are unlikely to recur. Finally, I am persuaded that Applicant and the company president are serious businessmen, they were embarrassed by the 2010 incident, they have a positive attitude toward security, they intend to cooperate with the DSS, and they are determined to operate the alarm company in compliance with the NISPOM. For all these reasons, the Guideline K security concerns, although serious, are mitigated.

2. Personal Conduct

Under Guideline E for personal conduct,[42] the suitability of an applicant may be questioned or put into doubt due to false statements and credible adverse information that may not be enough to support action under any other guideline. The overall security concern under Guideline E is:

> 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.[43]

---

[41] AG ¶ 35(a)–(c).

[42] AG ¶¶ 15–17 (setting forth the security concern and the disqualifying and mitigating conditions).

[43] AG ¶ 15.

The primary issue alleged in the SOR under Guideline E is that Applicant made deliberately false or misleading statements to the IS Rep during the formal inquiry in 2010. As noted in the findings of fact, the IS Rep did not appear as a witness at the hearing. This allegation is based on the paperwork prepared by the IS Rep; namely, the administrative inquiry and the culpability report.[44] In particular, the allegation is based on the IS Rep's account of how Applicant responded to questions and how his answers changed.[45] In considering this evidence, I note that common sense and experience teach that information often comes out in bits and pieces scattered across a conversation or interview. It is not unusual for people to relate information during a conversation, interview, or interrogation based on what questions are asked, how the questions are asked, how the questions are ordered or sequenced, etc. And as an interviewer obtains information, it is typical to repeat, rephrase, or refine questions to obtain a better understanding of the answers. Based on the record before me, I am unable to determine what happened during the interview with Applicant, and the paperwork is not enough to conclude Applicant made deliberately false or misleading statements. Accordingly, this matter is decided for Applicant.

The secondary issue alleged in the SOR under Guideline E is the cross reference to the Guideline K allegations. I have considered all the potential disqualifying conditions under Guideline E, and none apply to the Guideline K allegations. Assuming for the sake of argument that one or more disqualifying condition applies, the security concern is mitigated under the same rationale used to mitigate the concern under Guideline K. Accordingly, this matter is decided for Applicant.

Following *Egan* and the clearly-consistent standard, I have no doubts or concerns about Applicant's fitness or suitability for a security clearance. In reaching this conclusion, I weighed the evidence as a whole and considered if the favorable evidence outweighed the unfavorable evidence or *vice versa.* I also gave due consideration to the whole-person concept.[46] Having done so, I conclude that Applicant met his ultimate burden of persuasion to obtain a favorable clearance decision. This case is decided for Applicant.

Formal Findings

The formal findings on the SOR allegations are as follows:

Paragraph 1, Guideline K:	For Applicant
Subparagraphs 1.a–1.b:	For Applicant

[44] Exhibit 4.

[45] Exhibit 4 at 3.

[46] AG ¶ 2(a)(1)–(9).

Paragraph 2, Guideline E:	For Applicant
Subparagraphs 2.a–2.b:	For Applicant

Conclusion

In light of the record as a whole, it is clearly consistent with the national interest to grant Applicant eligibility for a security clearance. Eligibility for access to classified information is granted.

Michael H. Leonard
Administrative Judge