



**DEPARTMENT OF DEFENSE  
DEFENSE OFFICE OF HEARINGS AND APPEALS**



In the matter of: )  
)  
) ISCR Case No. 10-01852  
)  
)  
Applicant for Security Clearance )

**Appearances**

For Government: Fahryn E. Hoffman, Esq., Department Counsel  
For: Applicant: Kevin Sherlock, Esq.

January 20, 2012

**Decision**

COACHER, Robert E., Administrative Judge:

Applicant mitigated the security concerns under Guideline K, Handling Protected Information and Guideline E, Personal Conduct. Applicant’s eligibility for a security clearance is granted.

**Statement of the Case**

On May 16, 2011, the Defense Office of Hearings and Appeals (DOHA) issued Applicant a Statement of Reasons (SOR) detailing security concerns under Guideline K, Handling Protected Information and Guideline E, Personal Conduct. DOHA acted under Executive Order 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the adjudicative guidelines (AG), effective within the Department of Defense after September 1, 2006.

Applicant answered the SOR on July 22, 2011, and requested a hearing before an administrative judge. The case was assigned to me on October 4, 2011. DOHA issued a notice of hearing on October 31, 2011, with a hearing date of November 16, 2011. The hearing was held as scheduled. The Government offered Exhibits (GE) 1 through 4, which were admitted into the record without objection. Department Counsel's exhibit index was marked as Hearing Exhibit (HE) I. Applicant testified, offered one witness, and produced exhibits (AE) 1 through 17 that were admitted into the record without any objection. DOHA received the hearing transcript (Tr.) on November 29, 2011.

### **Findings of Fact**

In Applicant's answer to the SOR, she denied the allegations. After a thorough and careful review of the pleadings, testimony, and exhibits, I make the following findings of fact.

Applicant is 49 years old. She has been married for 29 years. She has one child. She has worked for a defense contractor since 2005. She is a security specialist. She has also held a secret clearance since 2005. She has some college.<sup>1</sup>

The allegations against Applicant include that she gave unauthorized access to classified areas to at least eight persons prior to their signing a nondisclosure agreement (NDA). Her action is alleged under both Guidelines K and E. Additionally, under Guideline E, it is alleged that she provided false or misleading information to her employer on September 17, 2008, when asked about her input of information into the Joint Personnel Adjudication System (JPAS) (SOR ¶¶ 1.a – 2.b).

Applicant began working for her current employer as a direct-hire employee in April 2005. She was hired as an industrial security specialist. She is currently the custodian for all classified information for the entire division. Her hiring supervisor described her as a top performer who far exceeds standards. He also described the many awards she received in the security field, such as an engineering security excellence award. She was one of twelve who received the award out of 5,700 employees. This supervisor has spent most of his career dealing with classified information and is a retired chief master sergeant in the Air Force. He further relayed that Applicant takes her security duties very seriously. He described her as trustworthy, reliable, and worthy of holding a security clearance. He did say that he was unfamiliar with the specific issues that led to this hearing for Applicant.<sup>2</sup>

In 2007, Applicant remained with her employer, but moved to a location in another state. She described the security organization as lacking in overall management control. She also demonstrated that she was performing far more duties

---

<sup>1</sup> Tr. at 68; GE 1.

<sup>2</sup> Tr. at 28-33; GE 1.

than was optimal for her position and that currently there more people performing all those duties. She also was not trained in many of the duties she needed to perform. As part of her security duties, she inputted the dates when employees signed their NDA. According to Applicant, she was trained by her predecessor to enter all information into JPAS the day that it came into their control. As a result, NDA dates were entered when employees had not yet actually signed their NDAs. The facilities security officer (FSO) became aware of this practice and discovered that at least eight employees had their NDA signature dates entered into JPAS before they actually signed the document. The National Industrial Security Program Operating Manual (NISPOM) requires that all cleared employees must sign a NDA before being granted access to classified information. The FSO conducted an investigation and concluded that the eight people gained access to closed areas and had access to classified networks prior to signing their NDAs. Applicant claimed that even if JPAS showed that their NDAs had been signed when they were not, these people would not have had access to classified information. She further explained that a security badge was necessary to gain access to the areas in question. The only way to get access was to get a security briefing which included signing the NDAs. I find Applicant's testimony explaining the process credible and more helpful than the unsigned security incident report prepared by the FSO. Although the incident report states that the eight people gained access to classified areas and information, it does not give any specifics about this improper access, such as when it occurred, what information was accessed by whom, or what remedial action was taken. Once Applicant was informed of the proper way to input the NDA dates into JPAS, there were no further problems. Applicant has never had a security issue since then. The FSO no longer works for the company.<sup>3</sup>

In September 2008, the FSO interviewed Applicant about her NDA date entries. Applicant explained that she entered the data as she was trained to do. Applicant admitted to telling this to the FSO. The FSO's incident report states that later in the interview, Applicant recanted her statement that she was trained to enter the dates early and further explained that she entered the dates early hoping the employees would come by and pick up their access badges. The report makes reference to an email from Applicant that describes her process for granting access; however, the email is not included in the report. Applicant denied making the recantation or of making any false or misleading statements to the FSO in September 2008. Later, in Applicant's January 2010 statement to a defense investigator, she again admitted to inputting the NDA dates based upon her training, but did not make any mention of doing so hoping the employees would come by to pick up their badges. I find Applicant's testimony to be consistent with her earlier statement to a defense investigator and of greater weight than the FSO's unsigned incident report.<sup>4</sup>

Applicant presented evidence of numerous awards, certificates, and recognition for her superior work in the security area. She was deemed a "Security Superstar" in

---

<sup>3</sup> Tr. at 47-48, 50-51, 53-57, 59, 89; GE 3-4; AE 15-16.

<sup>4</sup> Tr. at 56, 59; GE 2-3.

2009 by the company's director of global security. She was selected as employee of the month on two occasions. Additionally, through her efforts, the company received a commendable Defense Security Service (DSS) security rating, a first for the company. Her performance appraisals indicate that she is an outstanding employee. Overall, the documents submitted reflect professional service, leadership, high integrity, and outstanding performance over the course of Applicant's career.<sup>5</sup>

### **Policies**

When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the adjudicative guidelines. In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially disqualifying conditions and mitigating conditions, which are used in evaluating an applicant's eligibility for access to classified information.

These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, these guidelines are applied in conjunction with the factors listed in the adjudicative process. The administrative judge's overarching adjudicative goal is a fair, impartial, and commonsense decision. According to AG ¶ 2(c), the entire process is a conscientious scrutiny of a number of variables known as the "whole-person concept." The administrative judge must consider all available, reliable information about the person, past and present, favorable and unfavorable, in making a decision.

The protection of the national security is the paramount consideration. AG ¶ 2(b) requires that "[a]ny doubt concerning personnel being considered for access to classified information will be resolved in favor of national security." In reaching this decision, I have drawn only those conclusions that are reasonable, logical, and based on the evidence contained in the record.

Under Directive ¶ E3.1.14, the Government must present evidence to establish controverted facts alleged in the SOR. Under Directive ¶ E3.1.15, an "applicant is responsible for presenting witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by applicant or proven by Department Counsel, and has the ultimate burden of persuasion to obtain a favorable security decision."

A person who seeks access to classified information enters into a fiduciary relationship with the Government predicated upon trust and confidence. This relationship transcends normal duty hours and endures throughout off-duty hours. The Government reposes a high degree of trust and confidence in individuals to whom it grants access to classified information. Decisions include, by necessity, consideration of the possible risk that an applicant may deliberately or inadvertently fail to safeguard classified information. Such decisions entail a certain degree of legally permissible

---

<sup>5</sup> AE B-C.

extrapolation as to potential, rather than actual, risk of compromise of classified information.

Section 7 of Executive Order 10865 provides that decisions shall be “in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned.” See *also* EO 12968, Section 3.1(b) (listing multiple prerequisites for access to classified or sensitive information).

## **Analysis**

### **Guideline K, Handling Protected Information**

AG ¶ 33 expresses the security concern pertaining to handling protected information:

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.

I have considered all the Handling Protected Information disqualifying conditions under AG ¶ 34 and determined the following apply:

(a) deliberate or negligent disclosure of classified or other protected information to unauthorized persons, including but not limited to personal or business contacts, to the media, or to persons present at seminars, meetings, or conferences; and

(g) any failure to comply with rules for the protection of classified or other sensitive information.

Although the record lacks evidence indicating that there was an actual unauthorized disclosure, the possibility existed that eight people were given access to classified areas or information. Applicant admitted putting in NDA dates into JPAS before the employees signed the agreements because she was trained by her predecessor to do it that way. Both AG ¶¶ 34(a) and (g) apply.

All the mitigating conditions for Handling Protected Information under AG ¶ 35 were considered and the following were found relevant under these circumstances:

(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; and

(c) the security violations were due to improper or inadequate training.

Applicant's actions can be considered remote since they occurred in September 2008. She has not experienced another security issue since that time. On the contrary, she has been recognized by her company for her outstanding service in the security area on numerous occasions. She provided convincing evidence to show that sufficient time has passed since the incident, that any security issues are unlikely to recur, and that her current reliability, trustworthiness, and good judgment are not in doubt. AG ¶ 35(a) applies.

Once she was informed that she was inputting the NDA information incorrectly, she did not have any further incidents. Although her job, from that point on, did not involve making JPAS inputs, she was working on a regular basis with classified information and has not had any security issues. She has responded favorably to counseling. AG ¶ 35(b) applies.

Applicant credibly testified that she was not given proper training in the area of inputting NDA information into JPAS. She was actually trained to improperly input the information. Once discovered, corrections were made. She presented sufficient evidence to establish her training in this area was improper or inadequate. AG ¶ 35(c) applies.

### **Guideline E, Personal Conduct**

AG ¶ 15 expresses the security concern for personal conduct:

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.

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

(b) deliberately providing false or misleading information concerning relevant facts to an employer; and

(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.

Applicant credibly testified that she did not give false or misleading information concerning inputting the NDA data to her employer when she was asked about it in September 2008. Her testimony is consistent with her previous statement given to an investigator. The Government did not establish a deliberate falsification or misleading statement. AG ¶ 16(b) does not apply.

For the reasons stated under the Guideline K analysis above, the cross-alleged allegation at SOR ¶ 1.b is not supported by the evidence, because Applicant's record supports a whole-person assessment of good judgment, trustworthiness, reliability, and other characteristics indicating she will properly safeguard protected information. AG ¶ 16(c) does not apply.

### **Whole-Person Concept**

Under the whole-person concept, the administrative judge must evaluate an applicant's eligibility for a security clearance by considering the totality of the applicant's conduct and all the circumstances. The administrative judge should consider the nine adjudicative process factors listed at AG ¶ 2(a):

- (1) the nature, extent, and seriousness of the conduct;
- (2) the circumstances surrounding the conduct, to include knowledgeable participation;
- (3) the frequency and recency of the conduct;
- (4) the individual's age and maturity at the time of the conduct;
- (5) the extent to which participation is voluntary;
- (6) the presence or absence of rehabilitation and other permanent behavioral changes;
- (7) the motivation for the conduct;
- (8) the potential for pressure, coercion, exploitation, or duress; and
- (9) the likelihood of continuation or recurrence.

Under AG ¶ 2(c), the ultimate determination of whether to grant eligibility for a security clearance must be an overall commonsense judgment based upon careful consideration of the guidelines and the whole-person concept.

I considered the potentially disqualifying and mitigating conditions in light of all the facts and circumstances surrounding this case. I considered that Applicant's actions occurred over three years ago without recurrence since then. I considered the lack of training, in fact, improper training, she received that led to the improper JPAS inputs. I also considered that she has been recognized for her outstanding work in the security field on numerous occasions since this incident. All of which demonstrate her permanent behavior changes toward security issues and the unlikeliest chance of

recurrence. Applicant met her burden and provided sufficient evidence to mitigate the security concerns.

Overall the record evidence leaves me without questions or doubts about Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude Applicant mitigated the security concerns arising under Guideline K, Handling Protected Information and Guideline E, Personal Conduct.

### **Formal Findings**

Formal findings for or against Applicant on the allegations set forth in the SOR, as required by section E3.1.25 of Enclosure 3 of the Directive, are:

Paragraph 1, Guideline K:	FOR APPLICANT
Subparagraph 1.a:	For Applicant
Paragraph 2, Guideline E:	FOR APPLICANT
Subparagraphs 2.a-2.b:	For Applicant

### **Conclusion**

In light of all of the circumstances presented by the record in this case, it is clearly consistent with the national interest to grant Applicant eligibility for a security clearance. Eligibility for access to classified information is granted.

---

Robert E. Coacher  
Administrative Judge