DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 12-04737
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Daniel Crowley, Esq., Department Counsel
For Applicant: *Pro se*

08/26/2013

_____

Decision

_____

O'BRIEN, Rita C., Administrative Judge:

Based on a review of the pleadings, testimony, and exhibits, I conclude Applicant has not mitigated the security concerns related to handling protected information and personal conduct. Accordingly, her request for a security clearance is denied.

Statement of the Case

On June 4, 2013, the Department of Defense (DOD) issued to Applicant a Statement of Reasons (SOR) citing security concerns under Guidelines K (handling protected information) and E (personal conduct) of the Adjudicative Guidelines (AG).[1] In her June 12, 2013 Answer to the SOR, Applicant admitted the three allegations under Guidelines K and E, and requested a hearing before an administrative judge of the Defense Office of Hearings and Appeals (DOHA). On July 25, 2013, DOHA issued a Notice of Hearing, and I convened the hearing on July 30, 2013. I admitted two

[1] Adjudication of the case is controlled by Executive Order 10865, as amended; DOD Directive 5220.6 (Directive), as amended; and the Adjudicative Guidelines, which supersede the guidelines listed in Enclosure 2 to the Directive. They apply to all adjudications or trustworthiness determinations in which an SOR was issued on or after September 1, 2006.

Government exhibits (GE 1-2), and three Applicant exhibits (AE A-C).[2] DOHA received the transcript on August 7, 2013.

Procedural Ruling

When notified by Department Counsel that her hearing was about to be scheduled, Applicant requested that it be held as soon as possible. I granted her request, and the written Notice of Hearing was issued five days before the hearing. During the hearing, Applicant affirmatively waived her right under §E3.1.8 of the Directive to receive notice 15 days before the hearing date. (Tr. 8-9)

Findings of Fact

Applicant's admissions in response to the SOR are incorporated as findings of fact. After a thorough review of the pleadings, Applicant's response to the SOR, and the evidence, I make the following additional findings of fact.

Applicant is 30 years old. She holds bachelor's and master's degrees in criminal justice, completed in 2005 and 2010, respectively. She is single and has no children. She served as an enlisted member of the Air Force from 2006 to 2010. She completed training as an imagery analyst in February 2007. That year, she was granted a top secret security clearance with special accesses, while in the Air Force. In December 2010, she began her current position as an imagery analyst for a defense contractor. Applicant had security training during her military career, as well as mandatory computer-based security training when she worked for the contractor. (GE 1; Tr. 18-24, 36)

In spring 2007, Applicant was stationed at an Air Force base for her first assignment. She was taking career development courses (CDCs) to qualify for her position. The course materials were classified secret, and she was required to study them in a sensitive compartmented information facility (SCIF). She studied in her off-duty hours. On two occasions, Applicant decided to remove several pages from one of the course binders and take them home to study, where she would be more comfortable. Because of her training in the proper handling of classified material, Applicant knew that what she did was prohibited. (GE 2; Tr. 24-30, 37, 39-40)

In her interrogatory, Applicant noted, "However, once I had the materials in my possession, guilt does not even begin to describe what I felt." She testified she kept the materials at home between one and four weeks. She was afraid of being caught if she brought the material back to the SCIF. She stated in her interrogatory, "I knew I had to destroy them." She burned the material in her bathtub, and flushed the ashes down the drain. In her Answer, Applicant stated that her actions were not done "with malicious

[2] At the hearing, Applicant had an unsigned copy of one of her character reference letters. She provided a signed copy after the hearing. Department Counsel had no objection to the signed version, which was the same as the unsigned version, other than the writer's changed contact information. Both versions are included in AE B.

intent" but represented a "severe lapse in judgment." She did not report her actions to her command, security officer, coworkers, family, or friends. (GE 2; Tr. 24-30, 37, 39-44)

Four years later, in October 2011, Applicant underwent a polygraph examination for her position with a defense contractor. She disclosed her 2007 removal, storage, and destruction of classified information. During her December 2011 security interview, Applicant disclosed her actions to the agent. She also stated that she, "felt as if people knew" what she did, including her security officer. However, no one confronted her about the missing classified material. As of the hearing date, she had told only the security interviewer and the polygrapher. She did not report her actions because "I didn't know what to say." (GE 2; Tr. 30-31, 35-36, 40, 44)

On about five occasions between 2007 and 2011, Applicant inadvertently carried her cell phone or camera into a secure area. She had received training that included the prohibition on carrying such items into a SCIF. When she realized she had the items with her, she took them out of the secure area and placed them in a locker, but did not report the incidents. Most of the incidents occurred while she served in the military. In her interrogatory response, she noted that these incidents were not done with malicious intent. She did not report these incidents because "I was not sure what to say or who I would report it to." (GE 2; Tr. 27-28, 37-39)

Applicant received a Certificate of Recognition for her outstanding performance for the federal agency that she supported from 2006 to 2013. A friend of nine years described her honesty and "tremendous integrity." The chief of the branch she supports described her as "one of the best employees I have ever had" and noted her technical proficiency, ethics, and personal integrity. He opined that she could be trusted with the nation's most sensitive information. Her manager for the past 18 months described her as a dedicated professional who has ". . . worked with classified information, and to the best of my knowledge, has done this while always upholding all of the rules and regulations for safeguarding such information. I certainly believe that she is trustworthy and capable of handling classified information." The commander of Applicant's squadron, in a January 2010 letter, recommended Applicant as a remarkably talented and intelligent leader. He described her as "brilliant" in her "critical position" exploiting combat-related intelligence. None of the writers who submitted references are aware of Applicant's security violations. (AE A-C)

Policies

Each security clearance decision must be a fair and commonsense determination based on examination of all available relevant and material information, and consideration of the pertinent criteria and adjudication policy in the AG.[3] Decisions must also reflect consideration of the factors listed in ¶ 2(a) of the Guidelines, commonly referred to as the "whole-person" concept. The presence or absence of a disqualifying or mitigating condition does not determine a conclusion for or against an applicant.

[3] Directive. 6.3.

However, specific applicable guidelines are followed whenever a case can be measured against them as they represent policy guidance governing the grant or denial of access to classified information. In this case, the pleadings and the information presented by the parties require consideration of the security concerns and adjudicative factors addressed under Guidelines K and E.

A security clearance decision is intended only to resolve whether it is clearly consistent with the national interest[4] for an applicant to either receive or continue to have access to classified information. The Government bears the initial burden of producing admissible information on which it based the preliminary decision to deny or revoke a security clearance for an applicant. Additionally, the Government must be able to prove controverted facts alleged in the SOR. If the Government meets its burden, it then falls to the applicant to refute, extenuate, or mitigate the Government's case.

Because no one has a "right" to a security clearance, an applicant bears a heavy burden of persuasion.[5] A person who has access to classified information enters into a fiduciary relationship with the Government based on trust and confidence. Therefore, the Government has a compelling interest in ensuring that each applicant possesses the requisite judgment, reliability, and trustworthiness of one who will protect the national interests as his or his own. The "clearly consistent with the national interest" standard compels resolution of any reasonable doubt about an applicant's suitability for access in favor of the Government.[6]

Analysis

Guideline K, Handling Protected Information

AG ¶ 33 expresses the security concern under Guideline K:

> 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 the disqualifying conditions under AG ¶ 34, especially the following:

> (b) collecting or storing classified or other protected information at home or in any other unauthorized location;

[4] *See Department of the Navy v. Egan*, 484 U.S. 518 (1988).

[5] *See Egan,* 484 U.S. at 528, 531.

[6] *See Egan;* Adjudicative Guidelines, ¶ 2(b).

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

(h) negligent or lax security habits that persist despite counseling by management; and

(i) Failure to comply with rules or regulations that results in damage to the national Security, regardless of whether it was deliberate or negligent.

.

In spring 2007, while serving as an enlisted member of the Air Force, Applicant removed secret material from a SCIF, transported it to her home, and stored it there for one to four weeks. During that period, the material was not secure and was vulnerable to disclosure. Fearing that returning the material to the SCIF would result in discovery of her violation, Applicant destroyed the classified material. She had received security training and was aware that she was violating security regulations. Despite this knowledge, she deliberately failed to comply with the rules. AG ¶¶ 34(b) and (g) apply. AG ¶ 34(h) partially applies because Applicant was negligent on the five occasions when she carried a cell phone or camera into a secure area. No counseling was involved, because Applicant did not inform her supervisor of these violations. AG ¶ 34(i) does not apply because the record contains no evidence regarding damage to the national security that resulted from Applicant's actions.

AG ¶ 35 provides the following conditions that could mitigate security concerns:

(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 did not occur under unusual circumstances, but rather in the regular course of her duties. She committed a security violation that continued for one to four weeks. Although the events occurred six years ago, the serious nature of the violation outweighs the lack of recency. Applicant's failure to follow restrictions regarding her cell phone and camera demonstrate a lax attitude toward her security responsibilities. Her actions reflect poorly on her reliability, trustworthiness, and judgment. AG ¶ 35(a) does not apply. In addition, Applicant’s violations regarding classified material and her cell phone did not stem from inadequate training. AG ¶ 35(c) does not apply.

As to AG ¶ 35(b), although Applicant has not received remedial training, her character references indicate that she is currently conscientious about security responsibilities. However, these evaluations must be viewed in light of the fact that none of the writers are aware of her security violations or her lack of candor in disclosing them. Applicant receives limited mitigation under AG ¶ 35(b).

Guideline E, Personal Conduct

AG ¶ 15 expresses the security concern pertaining to 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….

AG ¶ 16 describes conditions that could raise a security concern, including the following relevant condition:

> (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: (1) untrustworthy or unreliable behavior; . . . (3) a pattern of dishonesty or rule violations… ; and
>
> (e) personal conduct, or concealment of information about one's conduct, that creates a vulnerability to exploitation, manipulation, or duress, such as (1) engaging in activities which, if known, may affect the person's personal, professional, or community standing, or (2) while in another country, engaging in any activity that is illegal in that country or that is legal in that country but illegal in the United States and may serve as a basis for exploitation or pressure by the foreign security or intelligence service or other group.

In 2007, Applicant deliberately failed to inform anyone in her command, including her security officer, that she had stored secret data in her home for one to four weeks, or that she had destroyed classified material. In 2010, after her employment by a defense contractor, she again decided not to inform her supervisor or facility security officer of her violations. Applicant's conduct showed poor judgment and lack of candor. Her concealment of the information for four years demonstrates a pattern of rule violations, and left her vulnerable to exploitation because exposure could have affected her military career. AG ¶¶ 16(d) and (e) apply.

AG ¶ 17 provides conditions that could mitigate security concerns under the Personal Conduct guideline:

> (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;
>
> (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; and
>
> (e) the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress.

As discussed under Guideline K, Applicant's conduct occurred during the regular course of her duties, not in unique circumstances. Her violations were not minor, because they involved exposing secret data to disclosure. Although they are not recent, their gravity outweighs the lack of recency. AG ¶ 17(c) does not apply.

Applicant realizes the serious nature of her conduct. Although there is no record evidence of counseling, she is genuinely remorseful for her actions. There is no evidence that she has violated security regulations since 2007, and it is highly unlikely that she will engage in such behavior in the future. AG ¶ 17(d) applies.

However, AG ¶ 17(e) cannot be applied because, as of the hearing date, Applicant had failed to reveal her conduct to anyone since her disclosure to the security interviewer and polygrapher in 2011. Without such disclosure, she remains vulnerable to exploitation. Applicant's security violations, and failure to disclose them, raise doubts about her reliability and judgment, and outweigh the mitigation under AG ¶ 17(d).

Whole-Person Concept

Under the whole-person concept, an administrative judge must evaluate an applicant's security eligibility by considering the totality of the applicant's conduct and all the relevant circumstances. I have evaluated the facts presented and have applied the appropriate adjudicative factors under the cited guidelines. I have also reviewed the record before me in the context of the whole-person factors listed in 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.

AG ¶ 2(c) requires that the ultimate determination of whether to grant a security clearance be an overall commonsense judgment based upon careful consideration of the guidelines and the whole-person concept. Under the cited guidelines, I considered the potentially disqualifying and mitigating conditions in light of all the facts and circumstances surrounding the case.

Applicant displayed lax security habits by repeatedly bringing her cell phone or camera in a secure area. However, her most serious violation occurred when she deliberately removed classified material from a SCIF and stored it for one to four weeks in her home, where it was not secure and was subject to disclosure. She credibly testified that she was immediately aware of the gravity of her acts, and felt guilty and remorseful. Applicant was 24 years old at the time, and her youth and inexperience undoubtedly played a part in her decisions. However, she was also an intelligent woman who had been trained in security procedures and regulations. Instead of returning the material and admitting her violations, she compounded the violation by burning the classified material, and concealing her conduct from her command and her employer for years. The fact that she still has not been candid with her employer about her past conduct raises concerns. For all these reasons, I conclude Applicant has not mitigated the cited security concerns. A fair and commonsense assessment of the available information bearing on Applicant's suitability for a security clearance shows she has not satisfied the doubts raised. Such doubts must be resolved in favor of the Government.

Formal Findings

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

Paragraph 1, Guideline K	AGAINST APPLICANT
Subparagraphs 1.a – 1.b	Against Applicant
Paragraph 2, Guideline E	AGAINST APPLICANT
Subparagraph 2.a	Against Applicant

Conclusion

In light of all of the foregoing, it is not clearly consistent with the national interest to allow Applicant access to classified information. Applicant's request for a security clearance is denied.

RITA C. O'BRIEN
Administrative Judge