DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 09-02694
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Franciso Mendez, Esq., Department Counsel
For Applicant: *Pro se*

May 3, 2010

Decision

RICCIARDELLO, Carol G., Administrative Judge:

Applicant mitigated the Government's security concerns under Guideline K, Handling Protected Information, Guideline M, Use of Information Technology Systems, and Guideline E, Personal Conduct. Applicant's eligibility for a security clearance is granted.

On October 8, 2010, the Defense Office of Hearings and Appeals (DOHA) issued to Applicant a Statement of Reasons (SOR) detailing the security concerns under Guidelines K, M, and E. The action was taken 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).

Applicant answered the SOR in writing on December 10, 2009, and requested a hearing before an administrative judge. The case was assigned to me on March 13, 2010. DOHA issued a Notice of Hearing on March 23, 2010. I convened the hearing as

scheduled on April 13, 2010. The Government offered Exhibits (GE) 1 through 3. Applicant did not object and they were admitted. Applicant testified on his own behalf. He did not offer any exhibits. DOHA received the hearing transcript (Tr.) on April 21, 2010.

Procedural Matters

Department Counsel moved to amend SOR ¶¶ 1.b and 1.c, by deleting the date December 2005 and inserting the date October 2006. Applicant had no objection and agreed to proceed with the hearing. The motion was granted.

Findings of Fact

Applicant admitted all of the allegations in the SOR. After a thorough and careful review of the pleadings, exhibits, and testimony, I make the following findings of fact.

Applicant is 32 years old. He graduated from high school in 1996 and attended college after high school, but did not earn a degree. He is presently taking college courses to complete his degree. He married in 2000 and divorced in 2002. He remarried in 2004, and he and his wife have two children, ages three and two. He works in the information technology field for a federal contractor.[1]

Applicant enlisted in the Army in 2000 and was honorably discharged in October 2006. While serving in the Army, he initially held a Secret security clearance and later it was upgraded to a Top Secret security clearance with access to sensitive compartmented information (SCI). Due to the nature of Applicant's job in the Army, all documents at the facility where he worked were required to be stamped "secret." Sometime in 2004, Applicant was on medical leave for approximately six weeks. He brought work home so he could stay current on his duties. While at work, he stamped a document "secret" as required by the command's protocol. He took the document home. In October 2006, while on terminal leave pending his discharge, he found the document. He believed it did not contained material that should have been classified information and he shredded it at his home. He did not inform anyone in the Army that he took the document home or that he shredded it. Later that same month he was interviewing for a new job. He was required to take a polygraph. During the interview prior to the polygraph, he revealed to the investigator that he had shredded the document and provided the above explanation for his actions. Applicant fully understood that he should have reported that he had the document and should not have shredded it. The document was not properly stored at his home. There is no evidence any information was compromised.[2]

Applicant was to return a week after his polygraph interview for a follow-up polygraph. While at home, he searched his memory to recall if he had violated any other

[1] Tr. 51-60, 78-82.

[2] Tr. 19-28, 51, 84-87.

security rules. When he returned a week later to be polygraphed a second time, he disclosed that on one occasion he made a copy of a classified document on a non-secure printer. He took responsibility for his actions. The reason for his actions was because the secure printer was broken and the command was busy preparing for a high-level official. He was in a hurry and took the action for expediency. He did not report his action until the polygraph.[3]

Applicant admitted that in 2006, while on duty, he had authorized access to government computers. He was required to access certain files as part of his duties. While he was performing his duties, he noticed that a personal file that he had authorized access to had a file named "resume." He was not authorized to open the personal resume file, but he did and made a copy of the resume to use as an example for his own resume. He then did a search to see if any other personal files might have resumes. He located a couple and made copies. His intention was not to gain personal information, but rather to use the others' resumes to assist in creating his own. He knew he should not have accessed coworkers' resumes.[4]

Applicant admitted while he was on duty one night, he swapped a CD drive on a classified SIPR computer with a DVD drive and downloaded unauthorized software. His intention was to watch a movie on the computer. His supervisor observed him and asked what he was doing and he was told to stop. He did as he was told and deleted the software from the SIPR computer and returned the CD drive. No other action was taken.[5]

Applicant learned sometime in 2007 that his security clearance was revoked by another Government agency. This occurred after he disclosed the above information in conjunction with his polygraph examination. He was not aware of which agency it was, but confirmed he was advised of the revocation.[6]

Applicant went to nonjudicial punishment on two occasions while serving in the Army. The first one occurred in 2001, when he was still in training and in a restricted environment. He was "absent without official leave" for approximately 24 hours. His wife came to his duty station and they had an argument. He was reduced in grade, and was awarded restriction, and extra duties. In 2005, he went to nonjudicial punishment for "neglect of duty." Applicant acknowledged he pleaded guilty to the offense. He was required to follow up on an inventory and did not. He stated he was not aware that he was required to follow up on the inventory, but decided not to contest the allegation. He was reduced in grade and received extra duties.[7]

[3] Tr. 28-30, 61, 89.

[4] Tr. 30-34, 62-67.

[5] Tr. 34-37, 67-71.

[6] Tr. 37-38, 76.

[7] Tr. 38-47, 72-76.

Applicant took full responsibility for his actions and did not offer excuses. He worked in an environment that was in constant contact with classified information. He worked in a secure building that required special access for those entering. He explained that the environment he was in had become lax about security rules. He understands the serious ramifications of his lax conduct. He stated that after serious reflection about his actions, he truly grasps the magnitude and the negative implications of the number of infractions he committed. He understands that although he was committed to security awareness, he made personal compromises for convenience. He understood that the only assurance he could provide that he would not repeat his actions was his solemn promise. He stated that if he is trusted again with a security clearance he would not betray that trust. I found Applicant sincere and credible.[8]

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 considered 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. Likewise, I have avoided drawing inferences grounded on mere speculation or conjecture.

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

[8] Tr. 48-50, 88-91.

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 the applicant may deliberately or inadvertently fail to safeguard classified information. Such decisions entail a certain degree of legally permissible 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.

AG ¶ 34 describes conditions that could raise a security concern and may be disqualifying. I have specifically considered the following:

> (b) collecting or storing classified or other protected information at home or in any other unauthorized location; and
>
> (g) any failure to comply with rules for the protection of classified or other sensitive information.

Appellant brought home a document classified "secret." He stored it at his residence for approximately two years and then destroyed it without reporting his actions. He made a copy of a classified document on an unclassified copy machine. I find both of the above disqualifying conditions apply.

I have considered all of the mitigating conditions under AG ¶ 35, and I have especially considered the following:

> (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 currently reliability, trustworthiness, or good judgment; and

(b) the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities.

Applicant admittedly became lax in following security procedures. He intentionally brought home a document that was marked secret. Applicant disobeyed the rules. Later when he found the document, he shredded it, and again did not follow the rules. He made a copy of a classified document on an unclassified copy machine for expediency. Applicant was in a secure environment where he dealt with classified documents regularly. He has had four and a half years to reflect on his conduct. He has matured and has a renewed appreciation for the seriousness of protecting classified information. He made mistakes and understands the importance of following all rules all the time. I do not believe Applicant will repeat his conduct. I am convinced he will be diligent in safeguarding classified information. I believe his lapse in judgment during this period of time is not indicative of his current reliability, trustworthiness and good judgment. I find Applicant has a positive attitude toward discharging his security responsibilities. Therefore, I find mitigating conditions AG ¶ 35(a) and ¶ 35(b) apply.

Guideline M, Use of Information Technology Systems

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

> Noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual's reliably and trustworthiness, calling into question the willingness or ability to properly protect sensitive systems, networks, and information. Information Technology Systems include all related computer hardware, software, firmware, and data used for the communication, transmission, processing, manipulation, storage, or protection of information.

AG ¶ 40 describes conditions that could raise a security concern and may be disqualifying. I have especially considered the following:

> (a) illegal or unauthorized entry into any information technology system or component thereof;
>
> (e) unauthorized use of a government or other information technology system; and
>
> (f) introduction, removal, or duplication of hardware, firmware, software, or media to or from any information technology system without authorization, when prohibited by rules, procedures, guidelines or regulations.

Applicant was authorized to view personal files that pertained to his duties. However, he was not authorized to view personal files for his personal use, which he did. Applicant replaced a CD drive with a DVD drive, and loaded software on a SIPR computer, so he could watch a movie. I find the above disqualifying conditions apply.

I have considered all of the mitigating conditions under AG ¶ 41 and especially considered the following:

> (a) so much time has elapsed since the behavior happened, or it happened under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment.

The same analysis as discussed above under Guideline K, applies to this guideline. There is no question Applicant's actions were wrong. He readily acknowledges he used poor judgment. It has been four years since he committed these violations. Applicant has matured and has a more responsible attitude towards the seriousness of complying with security rules. I find the above mitigating condition applies.

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. 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. I have especially considered the following:

> (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

> (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.

Applicant failed to properly report that he transported to and stored at his home a classified document and later destroyed it. He also failed to report he made a copy of a classified document on an unclassified computer. His security clearance was revoked in 2007 due to the security infractions and violations he committed. I find the above disqualifying conditions apply.

I have considered all of the mitigating conditions under AG ¶ 17 and especially considered the following:

> (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.

The analysis under Guideline K, Handing Protected Information, and Guideline M, Use of Information Technology Systems is the same for Guideline E, Personal Conduct. Applicant appreciates the seriousness of his conduct. He admits that he took shortcuts and became lax in following all of the security rules. It has been approximately four years since his conduct occurred. He does not take lightly what he did. I considered Applicant's statements, demeanor, and honesty in answering all of my questions. He demonstrated a mature and responsible attitude toward his conduct. He is committed to being scrupulously responsible. When asked what assurances he could give me that he would not exhibit similar behavior in the future, he candidly stated that all he could do was promise that if he was trusted again he would not betray the privilege. I found Applicant credible and sincere. I have considered the period of time since his last violation, his attitude, maturity, and renewed commitment to complying with all rules. I find Applicant's behavior is unlikely to recur and he has taken positive steps to ensure he does not become complacent. Therefore, I find the above mitigating conditions 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 have incorporated my comments under Guidelines K, M, 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. Applicant was young and immature when he committed security infractions and failed to comply with procedures. He understands the seriousness of his lax attitude. He has matured and acknowledged his actions. He did not make excuses and was honest when answering all of my questions. I do not believe Applicant is a security risk. I believe due to his youth and the office atmosphere he became complacent. I believe he will be diligent and is committed to complying with all regulations and procedures in the future. Overall the record evidence leaves me with no 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 the guidelines for Handling Protected Information, Use of Information Technology Systems, and 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
Subparagraphs 1.a-1.d:	For Applicant
Paragraph 2, Guideline M:	FOR APPLICANT
Subparagraphs 2.a-2.b:	For Applicant
Paragraph 3, Guideline E:	FOR APPLICANT
Subparagraphs 3.a-3.f:	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 a security clearance. Eligibility for access to classified information is granted.

_____
Carol G. Ricciardello
Administrative Judge