



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



In the matter of:)	
)	
SSN:)	ISCR Case No. 06-05503
)	
Applicant for Security Clearance)	

Appearances

For Government: Melvin A. Howry, Esquire, Department Counsel
For Applicant: *Pro se*

March 27, 2008

Decision

MASON, Paul J., Administrative Judge:

Applicant submitted her Security Clearance Application (SCA), on November 10, 2003. On November 7, 2007, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) detailing security concerns under the criminal conduct guideline (Guideline J) and the misuse of information technology systems guideline (Guideline M). The action was taken pursuant to 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 revised adjudicative guidelines (AG) promulgated by the President on December 29, 2005, and made effective within the Department of Defense for SORs issued on or after September 1, 2006.

Applicant submitted her notarized answer to the SOR on November 21, 2007. She elected to have her case decided administratively without a hearing. A copy of the government's File of Relevant Material (FORM, the government's evidence in support of the SOR) was sent to Applicant on January 22, 2008. Applicant received the FORM on January 30, 2008. Applicant's response was received by DOHA on February 22, 2008.

The case was assigned to this administrative judge on March 6, 2008. Based upon a review of the FORM, Applicant's eligibility for access to classified information is granted.

Findings of Fact

Applicant admitted the one allegation under paragraph 1 (criminal conduct) and one allegation under paragraph 2 (misuse of technology systems). Applicant is 32 years old and has been employed by a defense contractor since November 3, 2003. She seeks a security clearance.

Criminal Conduct

In 2001, according to Applicant's interview on July 3, 2007, with an investigator from the Office of Personnel Management (OPM), she was 25 years old, and struggling at a city university on the west coast. She became involved with 20 other individuals ("group") in the illegal uploading and downloading of pirated software. The reasons she became involved were "it was during her stupid college years," and "It was a way of meeting new people because she was bored." (interview with OPM, July 3, 2007) Some members of the group would upload software to servers, while others would download the software. The software consisted of games, software, and movies. The software was not sold outside the group. Applicant did not make a profit, and did not believe the group made a profit.

The Federal Bureau of Investigation (FBI) conducted a raid on Applicant's dorm room on December 11, 2001. Along with 20 other defendants, Applicant was indicted on June 11, 2002, for reproducing software for private gain, over a six-month period ending December 11, 2001. The indictment stated that all the defendants were members of the "group" (formed in 1997), and engaged in a conspiracy to illegally reproduce copyrighted material during a 180-day period ending on December 11, 2001, in violation of 17 U.S.C. 506(a)(2), and 18 U.S.C. 2319(c)(1). Applicant's overt acts in furtherance of the conspiracy occurred on July 5, 2001, when she accessed the primary server for the "group," and transferred pirated computer software, movies, and games.

On December 18, 2003, under the terms of a Plea Memorandum, Applicant entered her guilty plea with the United States (U.S.), because of her conduct on July 5, 2001. The Plea Memorandum supplies more details of the illegal enterprise, including the representation by the Government to recommend "the low end of any sentence within the applicable guideline range, as calculated above." (Plea Memorandum, December 18, 2003, p. 2) The conspiracy involved making available thousands of copyrighted software programs and games, exceeding a retail value of \$1,000,000.00, by uploading or downloading the software in violation of the copyrights. It was determined during the course of the investigation leading to the Plea Memorandum that the group had a hierarchy of responsibility as follows: (1) "council members" who determined the terms and conditions under which the "group" was to operate; (2) "site operators" who maintained the sites where the pirated software was located; (3) "couriers" who specialized in transferring the illegal software around on the Internet;

and, “members” who had achieved membership in the “group” but had no specific role in the hierarchy. The Assistant United States Attorney classified Applicant as a “member.” (Plea Memorandum, Facts to Support a Plea of Guilty, p. 9)

On July 11, 2007, Applicant was sentenced to one count of conspiracy, in violation of 18 U.S.C. 371. She received 36 months probation retroactive to December 18, 2003, the date that Applicant pled guilty. She also was assessed a \$1,000.00 fine.

In an attachment to her answer to the SOR, Applicant explained how her illegal conduct helped turn her life around, both academically and professionally. She stated:

In general, we tend to focus on the negative parts of a person’s life, yet, ignore what the person has done after they have made a mistake. The mistake that I made is stated in paragraph 1a in the Statement of Reasons. I admit my wrongdoing. Instead of making excuses or finding ways to deny my involvement, I pled guilty. I don’t regret what happened since it has changed my life for the better. However, I do apologize for what I did. Before it happened, I was struggling with school and struggling with my life. I was failing classes and I was close to academic probation.

Next, she explained in the attachment that after the police raided her dorm room in December 2001, she sank into a period of depression, where she basically felt sorry for herself. A few months later, she decided changes in her life were necessary, and she was the only person to effect change. Her grades began to improve. She stated:

On December 2003, I received my Bachelors’ degree in Computer Science. I have been working for [employer] for four years and enjoy what I do. A year ago I bought my first house. I feel that I turned a bad situation into something good. I have learned my lesson. I am more aware of what I do. I think before I act. It has been an emotional battle, but I know how to deal with it. I have faith that every thing will get better and that keeps me going.

Misuse of Technology Systems

On July 5, 2001, Applicant inappropriately accessed the primary file transfer protocol and transferred pirated software.

Character Evidence

On June 29, 2007, the Human Relations Generalist of Applicant’s employer authored a letter to the presiding judge describing Applicant’s character. The human relations official indicated that Applicant told him about her crime, her regret for becoming involved, and her assurance the behavior would never happen again. The official noted Applicant had a promising future based on (1) her dependability as an employee, and (2) her successful job performance.

Applicant's older sister recalled in a character statement dated February 12, 2008 (part of Applicant's response to the FORM), that while in college, Applicant had no direction, and was in an abusive relationship. The older sister was impressed by dramatic changes Applicant underwent following the offense by finishing college in December 2003, and beginning her career with her employer in November 2003. Applicant's younger sister wrote a character statement extolling the favorable changes Applicant made in finishing school in December 2003, and providing a positive impact at her job. Applicant also served as a mentor for several of her younger sister's high school classmates. A friend who met Applicant in church in September 2007 considers her a caring person.

Applicant's performance evaluations for 2005 through 2007 show her successful job performance. Applicant's scholastic transcript shows that she received her Bachelor's Degree in Computer Science on December 18, 2003.

Policies

When evaluating an applicant's suitability for a security clearance, the Administrative Judge must consider the revised adjudicative guidelines (AG). In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially disqualifying conditions and mitigating conditions, which are useful in evaluating an Applicant's eligibility for access to classified information.

These guidelines are flexible rules of law that are applied in conjunction with the general policy factors of 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 interest is the paramount consideration. AG ¶ 2b. 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, the Applicant is responsible for presenting "witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by applicant or proven by Department Counsel. . . ." The Applicant has the ultimate burden of persuasion as to obtaining 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 is not restricted to normal duty hours. Rather, the relationship is an-around-the-clock responsibility. The Government places a high degree of trust and confidence

in individuals to whom it grants access to classified information. Decisions include consideration of the possible risk the Applicant may deliberately or inadvertently fail to protect or 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.

Criminal Conduct (CC)

Criminal behavior casts doubts concerning a person's judgment and trustworthiness.

Misuse of Technology Systems (MTS)

Misuse or noncompliance with technology systems that raises questions about a person's willingness to properly protect computer systems.

Analysis

Criminal Conduct

The Government has established a case under the CC guideline. On December 18, 2003, Applicant pled guilty to knowingly conspiring with others to make available thousands of copyrighted programs, movies and games exceeding a value of \$1,000,000.00, a violation of 18 U.S.C. 371, conspiracy to commit copyright infringement. On June 29, 2007, Applicant was sentenced to three years probation, retroactive to December 18, 2003 (date of guilty plea). She was fined \$1,000.00. CC disqualifying condition (DC) 31.a. (*a single serious crime or multiple lesser offenses*) applies.

However, CC mitigating condition (MC) 32.a. (*so much time has elapsed since the criminal 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*) and CC MC 32.d. (*there is evidence of successful rehabilitation; including but not limited to the passage of time without recurrence of criminal activity, remorse or restitution, job training or higher education, good employment record, or constructive community involvement*) also apply. Almost seven years have passed since the crime occurred. Applicant has made spectacular changes in her life. In December 2003, she obtained her Bachelor's Degree in Computer Science, and, for the past four years, has been applying her knowledge as a software engineer with her employer. Based on her comments to the OPM investigator in July 2007 and her answer to the SOR, I am confident she will not repeat the poor judgment she demonstrated in 2001. The observations of the human relations official, her sisters and her friend, persuasively show me she understands the gravity of her behavior, and will never repeat this conduct in the future.

Even though Applicant was under the jurisdiction of the court until she was sentenced in July 2007, thereby subject to probable incarceration for violating any of the terms of the Plea Memorandum, the passage of at least six years without a recurrence of criminal activity is entitled to some mitigation. Also, based on her poignant statements about the criminal behavior being a watershed event in her life, I am convinced Applicant is remorseful for her exhibition of poor judgment. Rather than continuing to feel sorry for herself after the offense was uncovered in December 2001, she devoted reinvigorated attention to her academics and improved her scholastic average. Her perseverance paid off when she graduated from college in December 2003. Even before she graduated from school, her current employer clearly took a chance on her by granting her a position in November 2003. She has produced a good job performance for more than four years. She has also had an impact on her younger sister's high school friends by providing mentoring advice. On balance, the evidence produced under CC MC 32.a. and 32.d. warrant a finding for Applicant under the CC guideline.

Misuse of Technology Systems (MTS)

Under the MTS guideline, security concerns are raised over the noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual's reliability 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, manipulation, storage, or protection of information.

The Government has established its case under paragraph 2.a. Applicant knowingly used her computer to access the group's primary software site, and transferred pirated software. She admitted she violated the federal law of conspiracy to commit copyright infringement. She knew her behavior was wrong. MTS DC 40.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*) applies.

However, MTS MC 41.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*) applies. First, the Plea Memorandum addressing the details of the conspiracy shows that Applicant's participation in the criminal enterprise was minor as determined by the prosecuting U.S. Attorney. Second, her conduct has not been repeated since 2001. Third, in the six-year period after her apprehension, Applicant has used her time wisely by obtaining her degree in December 2003, and compiling a good job performance record over the last four years. The MTS guideline is resolved in Applicant's favor.

Whole Person Concept (WPC)

Applicant has met her burden of persuasion under the CC and MTS guidelines. The same conclusion is reached even after the circumstances of this case are evaluated in the context of the whole person. Rehabilitation begins with the person comprehending the seriousness of their conduct. Applicant has proven in her statement to OPM in July 2007 and her November 2007 answer to the SOR that she fully embraces the stupidity of her conduct in 2001. However, instead of flunking out of school, she rallied herself to finish school and find a job in her field. The documented success academically and professionally, translates to substantial behavioral changes that eliminate the chances of this kind of conduct recurring. Both the CC and MTS guidelines are found in Applicant's favor.

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 (Financial Considerations, Guideline F): FOR APPLICANT

Subparagraph 1.a. For Applicant

Paragraph 2 (Misuse of Technology Systems, Guideline M): FOR APPLICANT

Subparagraph 2.a. For Applicant

Conclusion

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

Paul J. Mason
Administrative Judge