DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 10-01397
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Richard Stevens, Esquire, Department Counsel
For Applicant: Ronald C. Syktus

September 29, 2011

Decision

CREAN, Thomas M., Administrative Judge:

Based on a review of the pleadings, exhibits, and testimony, eligibility for access to classified information is granted. Applicant mitigated the security concerns for criminal conduct and personal conduct.

Statement of Case

On January 5, 2009, Applicant submitted an Electronic Questionnaire for Investigations Processing (e-QIP) to retain a security clearance required for his employment with a defense contractor. After an investigation conducted by the Office of Personnel Management (OPM), the Defense Office of Hearings and Appeals (DOHA) issued an interrogatory to Applicant to clarify or augment potentially disqualifying information in his background. After reviewing the results of the background investigation and Applicant's response to the interrogatory, DOHA could not make the preliminary affirmative findings required to continue a security clearance. DOHA issued a Statement of Reasons (SOR), dated February 10, 2011, to Applicant detailing security concerns for financial considerations under Guideline F, criminal conduct under Guideline J, and personal conduct under Guideline 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) effective in the Department of Defense on September 1, 2006. Applicant received the SOR on February 24, 2011.

Applicant answered the SOR on March 8, 2011. He admitted all the allegations under the three security guidelines, and requested a hearing before an administrative judge. Department Counsel was prepared to proceed on April 8, 2011, and the case was assigned to me on May 19, 2011. DOHA issued a Notice of Hearing on June 9, 2011, for a hearing on June 22, 2011. I convened the hearing as scheduled. The Government offered 13 exhibits which I marked and admitted into the record without objection as Government Exhibits (Gov. Ex.). 1 through 13. Applicant and three witnesses testified. Applicant offered eight exhibits which I marked and admitted into the record as Applicant Exhibits (App. Ex.) A through H. DOHA received the transcript (Tr.) of the hearing on June 30, 2011.

Procedural issues

Applicant's attorney discussed the hearing date with Department Counsel prior to a Notice of Hearing being mailed on June 9, 2011. Applicant is entitled to 15 days advance notice of a hearing. (Directive E3.1.8.) Applicant was ready to proceed at the hearing on June 21, 2011, and he had sufficient time to prepare. Applicant, through his attorney, waived the 15-day notice requirement. (Tr. 6-7)

Department Counsel moved to withdraw the security concerns in the Statement of Reasons under Guideline F. Applicant did not oppose the motion. The motion was granted and the security concerns in Paragraph 3 of the SOR under Guideline F were withdrawn. (Tr. 43)

Findings of Fact

After a thorough review of the pleadings, exhibits, and transcript, I make the following essential findings of fact. Applicant admitted all SOR allegations with explanation. I make the following findings of fact.

Applicant is 52 years old and has been employed by a defense contractor for almost three years as a field electronic engineer. After Applicant graduated from high school, he enrolled in college for approximately three semesters. He then joined the Marine Corps and served eight years on active duty from 1979 until 1987. He received an honorable discharge. He then worked for defense contractors on the same contract from 1987 until 2003. He successfully held a security clearance since 1979, including access to top secret and sensitive compartmented information. He first married in January 1979 but divorced in February 1982. He married again in March 1982, and divorced in November 2004. During most of this time, he lived in State A. He separated from his second wife and moved to State B in 2003, while still working for a defense

contractor. After his divorce in November 2004, he married for the third time in November 2004. He moved to State C with his wife and children in November 2005 to open his own business. When that business failed, he returned to work with a defense contractor. He has three children or step-children living at home that he and his wife support. (T 9-11, 25-34; Gov. Ex. 1, e-QIP, dated January 5, 2009; Gov. Ex. 2, Applicant's Resume; App. Ex. C and D, DD 214, United States Marine Corps)

The criminal conduct and personal conduct security concerns arise from the same circumstances. After moving to State B and meeting his future wife in 2003, Applicant lived in her house with her and her children. At the request of his future wife, Applicant installed surveillance cameras in the house to observe her daughter. Also captured on the videos were two au pairs hired to care for Applicant's future wife's children. Applicant kept some of the videos on a computer hard drive. Applicant and his wife moved to State C for employment in November 2005, and sold the house. The new owners discovered the cameras and notified police. After the cameras were discovered, Applicant was arrested for child abuse but was found guilty of unauthorized video surveillance. He is on probation until February 2012. The two au pairs also sued Applicant and his wife for invasion of privacy. The criminal conduct security concern (SOR Paragraph 1) stems from the allegation of child abuse. The personal conduct security concerns (SOR Paragraph 2) arises from his conduct that led to the lawsuits filed by the two au pairs.

When Applicant moved to State B in 2003, his divorce from his second wife was pending and he met his future third wife. While they dated, he moved in with her and her family. His future wife had an 11-year-old daughter with psychological problems stemming from the accidental death of her father a few years before. The daughter had self-destructive tendencies. She was disruptive, moody, depressed, and had set fires. The daughter's psychologist told Applicant's future wife that she had to be observant of the daughter's behavior at all times. Applicant had experience while working for defense contractors with surveillance equipment. Applicant's future wife asked him to install surveillance cameras in the house so they could observe the daughter wherever she was in the house. He encountered no problems in installing the cameras. He initially installed cameras in the daughter's bedroom and bathroom. The cameras were activated by motion detection or by turning on lights. Any person entering those rooms would be observed. The images were recorded on a computer to be reviewed by Applicant or his future wife at a later time to determine if there was any inappropriate behavior. Their intent was to know what the daughter was doing and when she was doing it. There was extensive material so that it was difficult by a cursory review to determine if there were indications of behavioral problems for his wife's daughter. Applicant or his wife deleted many of the images, but also moved some to files for later detailed review. Usually, they were held only for a few days. Applicant and his wife did what they could to delete any images that did not show inappropriate or destructive behavior. He believed all images had been deleted from the files. (Tr. 45-48, 62-64, 66-73: Gov. Ex. 3, Response to Interrogatory, dated October 22, 2010)

During this time, Applicant's wife employed au pairs from foreign countries through a State Department approved agency. The legal employment contract required that the au pairs work for only one year. When Applicant first installed the cameras, one au pair was observed a few times in the bathroom. Images of the next au pair hired were also caught by the cameras. The cameras also caught the images of Applicant's underage niece who was visiting as well as the Applicant's wife's parents. As noted, the cameras were activated by motion or a light switch and caught the images of anyone in the rooms. The images on the computer were reviewed by Applicant or his wife. Some of the recordings were long, particularly if activated by the light switch and the lights were left on. Most of the recordings were deleted after review. Some were saved in a computer folder until they could be further reviewed. (Tr. 48-51; Gov. Ex. 4, Statement, dated July 23, 2010)

Applicant and his wife observed images of people other than the daughter. One of the au pairs was from Russia and Applicant and his wife were suspicious of her activities. They contacted an agent from the Naval Investigative Service (NIS) who suggested that they keep the au pair employed and continue to observe her and her activities. NIS agents requested Applicant to install additional video cameras to keep track of the au pair. They also requested them to monitor her phone calls and mail. Applicant and his wife complied with the requests. Additional cameras were installed in the basement. The au pair was finally terminated when she had an automobile accident with the children in the car. She was not authorized to drive the car. (Tr. 51-56)

When Applicant and his wife moved to State C in 2005, they sold their house which had the surveillance cameras. The cameras were not removed but Applicant informed his real estate agent of the cameras' locations. He does not believe the new owners were informed by the real estate agent of the presence of the cameras. When the new owners renovated the house, they discovered the cameras. They notified the police, who seized Applicant's computer equipment at his new home in State C. They discovered on the computer some images of Applicant's underage step-daughter, his underage niece, and the au pairs. Applicant claims the images were not taken or retained for prurient interests or reasons. He did not know the images were still on the computer. He only installed the cameras at the direction of either his wife or the NIS agents. He researched the law in State C when he moved in 2005 and knows that he cannot install surveillance cameras in his home in that state. (Tr. 55-62, 77-78)

Applicant was initially charged in State B with the felony of child sexual abuse for the images of the step-daughter and the niece. On the advice of his attorney, he pled guilty to two counts of the misdemeanor offense of camera surveillance. He was sentenced to one year for each count but placed on unsupervised probation for five years. His probation runs until February 2012. The police officer who investigated the incident located the two au pairs and notified them of the cameras and the images on the computer. The two au pairs sued Applicant and his wife for invasion of privacy. Applicant's wife was represented by her insurance company. Since Applicant and his wife were not married at the time the cameras were installed, the insurance company refused to represent Applicant or pay any judgment against him. The insurance

company settled the suits on behalf of the wife, paying each au pair $95,000. Applicant and his wife had no input into the decisions made by the insurance company. Since the insurance company was in charge and settled the case, Applicant had no choice but to pay his part of the suit. He paid one au pair $25,000, and the other $5,000. (Tr. 43-45, 55-61, 119-120; Gov. Ex. $, Statement, dated July23, 201; Gov. Ex. 5, Settlement Order, dated June 12, 2008; Gov. Ex. 6, settlement Order, dated January 22, 2008; Gov. Ex. 7, Police Incident Report, dated February 7, 2006, Gov. Ex. 8, Criminal Court Records, dated February 6, 2007; Gov. Ex. 9 Camera Surveillance Statute)

Applicant's wife testified that she is a supervisor in a military command and has worked for the Government for over 27 years. She has a security clearance. Her first husband died in an automobile accident in September 2000. Her daughter had psychological issues because her father's death. Her misbehavior continued for a few years both before and after she met Applicant. She took her to a child psychologist because of her misconduct. The psychologist told her to keep a careful watch on all of her daughter's activities. Someone set fire to her truck, so she determined that she had to more closely monitor the daughter. She was concerned that her daughter could engage in self-destructive behavior.

Applicant and his wife had been living together for about a year, so she requested him to install surveillance cameras in the home. They installed cameras in her room and in her bathroom. The bathroom camera was activated by the light switch and the room cameras by motion. They installed cameras in the downstairs bathroom used occasionally by her daughter. She knew Applicant and was not concerned about the images he would see of her daughter or others from the monitoring. She saw the same pictures and images Applicant saw. She knew Applicant was not looking at the images for prurient reasons. They did not look at the images on a daily basis but just when they suspected inappropriate behavior. After viewing the images, they deleted most but placed others in a folder on the computer until they had sufficient time to review the tapes. Sometimes they went back and reviewed the images and other times they did not. They would normally delete any images not involving her daughter. But if the images were of a long session and her daughter was not on the tapes initially, they would save the tapes in a folder for later review. Her daughter is now doing well. She seems to have gone beyond the self-destructive phase of her life and is no longer under psychological care. She is doing well in school and adjusted to her new environment when they moved in 2005. Applicant's wife does not see a reason to continue monitoring of the daughter's activities. They did not install cameras in their new home when they moved in 2005. (Tr. 94-104, 120-123)

Applicant's wife was frustrated with the handling of the criminal case against her husband. The police would not talk to her or Applicant about the facts. She wanted to fight the case since Applicant was assisting her with caring for her daughter. However, she could not afford the costs associated with contesting the case. The insurance company's attorney in the civil suit told her and Applicant that Applicant should take the plea bargain. She did not want to take it but left the decision to Applicant. (Tr. 104-109)

She was suspicious of one of the au pairs that she hired. The girl was from Russia and behaved strangely. Because of her security clearance, she talked to NIS agents who asked her to continue monitoring the girl. She told the agents she had surveillance cameras in the house The NIS agents asked her to keep the girl in her employment and monitor her activities with the cameras. They also tracked her computer usage and phone calls as requested by NIS. (Tr. 109-118)

Applicant's direct supervisor and manager testified that he has known Applicant since November 2008. He sees Applicant on a daily basis. Applicant is quiet and reserved but extremely intelligent. He has a great technical electronic expertise. His work is always top quality. He has talked with Applicant about the security allegations. He has no concerns about Applicant's ability to safeguard classified information. (Tr. 91-94)

The lead installer for Applicant's employer testified that he has known Applicant since 1993. He saw him on a daily basis until about 2000. They did not work together for about eight months at that time but kept in contact. When his company needed a good technician, he contacted Applicant and the company hired him. Applicant's reputation is very good. He is aware of the charges against Applicant and it does not affect his opinion of Applicant's security worthiness. He considers Applicant to be among the most trustworthy people he knows.

Applicant's performance reviews are excellent. They show he is regarded as an excellent technical instructor who understands complex security systems. He is rated as either meets or exceeds expectations. (App. Ex. A and B, Performance Reviews, 2010 and 2011)

Policy

When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the adjudicative guidelines (AG). In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially disqualifying conditions and mitigating conditions, which must be 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.

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 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 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.

Analysis

Criminal Conduct
Personal Conduct

The security concerns for criminal conduct and personal conduct in this case are raised from the same incident. The security concerns for both, as well as the disqualifying conditions and mitigating conditions, are so similar that they will be discussed together. Criminal activity creates doubt about a person's judgment, reliability, and trustworthiness. By its very nature it calls into question a person's ability or willingness to comply with laws, rules, and regulations (AG ¶ 30). Personal conduct involving questionable judgment, untrustworthiness, unreliability, or unwillingness to comply with rules and regulations can raise questions about an individual's reliability, trustworthiness, and ability to protect classified information. (AG ¶ 15)

At the request of his future wife, Applicant installed surveillance cameras in her home to monitor the potential self-destructive activities of his wife's daughter. The cameras captured images of people other than the daughter to include two au pairs employed by his wife. He was found guilty of improper use of surveillance cameras in violation of a state law, and sued by the two au pairs for invasion of privacy. The criminal conduct that creates a security concern is Applicant's improper use of surveillance cameras in violation of the state criminal statue. The personal conduct security concern is created by Applicant's conduct that led to lawsuits filed by the two au pairs as well as his criminal conduct.

Applicant's use of surveillance cameras in violation of state law is sufficient information to raise Criminal Conduct Disqualifying Conditions AG ¶ 31(a) (a single serious crime or multiple lesser offenses), and AG ¶ 31(c) (allegation or admission of criminal conduct, regardless of whether the person was formally charged, formally prosecuted or convicted). Applicant was placed on five years of unsupervised probation for his conviction. The probation runs until February 2012. This raises the disqualifying condition at AG ¶ 31(d) (individual is currently on parole or probations).

This criminal activity as well as the conduct leading to the lawsuits filed against Applicant by the au pairs for invasion of privacy for monitoring them by surveillance cameras raises Personal Conduct Disqualifying Conditions AG ¶ 16(c) (credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any 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 safe guard protected information); and AG ¶ 16(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: (3) a pattern of dishonesty or rule violations). Applicant's conduct leading to a conviction for violating state statutes and a judgment against him for invasion of privacy indicates conduct involving questionable judgment, untrustworthiness, unreliability, or unwillingness to comply with rules and regulations. This raises concerns about Applicant's reliability, trustworthiness, and ability to protect classified information.

I considered Criminal Conduct Mitigating Condition AG ¶ 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 Personal Conduct Mitigating Condition AG ¶ 19(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). I find that these mitigating conditions apply. The criminal and personal conduct activity took place in 2004 and 2005 when Applicant installed the surveillance cameras. Of more concern is that Applicant still had some of the images still on his computer. This led to the criminal and civil charges. Both Applicant and his wife testified that she asked him to install the cameras for a legitimate family reason. The mistake made by Applicant and his wife was that they did not insure that the images were deleted from the computer when no improper conduct by the daughter was found. They deleted most but not all of the images after reviewing them and finding no useful information. The failure to delete the images was careless but not done to satisfy any prurient interests in the images. Both Applicant and his wife had access to the

images and both viewed them. The circumstances leading to the criminal and civil charges were unusual and unique in that they were monitoring the daughter for self-destructive behavior. The monitoring happened over five to six years ago and has not recurred. The daughter now appears to be well and is not under medical care. It is unlikely that further monitoring will be required, so the capturing of images will not recur. Applicant and his wife did not install cameras when they moved to their present house.

I also considered for the personal conduct security concern AG ¶ 19(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 for the criminal conduct security concern AG ¶ 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). I find that these mitigating conditions apply. While Applicant and his wife both acknowledge that surveillance monitoring of the daughter was needed, but that they should have exercised greater care in how the system worked so that the system monitored only the daughter. They also acknowledged the need to be more careful in deleting and disposing of the images of others. They did not continue the monitoring when they moved and made a determination that they no longer needed to monitor the daughter for self-destructive actions. Applicant and his wife have not engaged in any further activities that could lead to criminal or personal conduct security concerns. Applicant presented sufficient information that he has learned from his experience with the surveillance cameras.

Applicant is still on probation which runs for approximately five more months. He was placed on unsupervised probation for five years or 60 months. He has served most of that probation without incident. I find no evidence that will remotely indicate that Applicant will not continue to successfully complete the period of probation. Applicant presented sufficient information to mitigate the security concerns for criminal and personal conduct.

Whole-Person Concept

Under the whole-person concept, an administrative judge must evaluate an applicant's eligibility for access to classified information 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 access to classified information 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 Applicant's eight years on active duty with the Marines and his honorable discharge. I considered that he is regarded as an excellent worker with excellent skills. I also considered he successfully held a security clearance for almost the entire time since 1979

Applicant installed surveillance cameras in his wife's home at her request to monitor her daughter for potential self-destructive activities. Unfortunately, images of other people were caught during the monitoring. Applicant and his wife disposed of or deleted most of the images. Some remained due to Applicant's or his wife's carelessness in deleting the images. The cameras were discovered by the new owners of the house, and a review of his computer showed the images were not totally deleted. Applicant was found criminally responsible for use of surveillance cameras, and sued by two of the people captured by the monitoring for invasion of privacy. Applicant's intent in installing the cameras was reasonable and appropriate. However, he was negligent in not ensuring the monitoring would not include people other than the intended target. He was further negligent by not ensuring that all images were deleted from a computer. Applicant has not installed cameras in his new home and he has not continued to monitor the daughter since she no longer has mental health issues. Applicant knows the requirement in his new location in State C against installing surveillance cameras to monitor the activity of others even in his own home. He has provided sufficient information to mitigate security concern for his criminal and personal conduct. Overall, the record evidence leaves me without questions or doubts as to Applicant's judgment, reliability, and trustworthiness. He established his suitability for access to classified information. Eligibility for access to classified information is granted.

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 J:	FOR APPLICANT
Subparagraph 1.a:	For Applicant
Paragraph 2, Guideline E:	FOR APPLICANT
Subparagraphs 2.a – 2.c:	For Applicant

Paragraph 3: Guideline F:	WITHDRAWN
Subparagraphs 3.a - 3.b	Withdrawn

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 access to classified information. Access to classified information is granted.

_____
THOMAS M. CREAN
Administrative Judge