DATE: June 30, 2006

In re:

SSN: ------------

Applicant for Security Clearance

ISCR Case No. 05-01964

DECISION OF ADMINISTRATIVE JUDGE

JUAN J. RIVERA

APPEARANCES

FOR GOVERNMENT

Richard Stevens, Esq., Department Counsel

FOR APPLICANT

Stanley E. Sacks, Esq.

SYNOPSIS

In 2002, Applicant proposed another contractor employee (renter) to enter into a false rental property agreement with an inflated rent payment to cover part of Applicant's home mortgage payment and a kickback to the renter. At the time, he was 26 years old, held a security clearance, and had worked for the government for approximately six years. Applicant failed to present sufficient evidence to mitigate security concerns raised by his personal conduct. Clearance is denied.

STATEMENT OF THE CASE

On September 21, 2005, the Defense Office of Hearings and Appeals (DOHA) issued Applicant a Statement of Reasons (SOR) alleging facts that raise security concerns under Guideline E (Personal Conduct). The SOR informed Applicant that, based on information available to the government, DOHA adjudicators could not make a preliminary affirmative finding that it is clearly consistent with the national interest to grant him access to classified information.[(1)]

Applicant answered the SOR (Answer) on October 14, 2005, and requested a hearing. The case was assigned to me on February 2, 2006. On March 22, 2006, I convened a hearing at which the government presented the testimony of one witness. I admitted government's exhibits (GE) 1-3, without objection. Applicant testified and presented the testimony of five witnesses and two exhibits that were admitted without objection and marked Applicant's exhibits (AE) 1 - 2. DOHA received the transcript (Tr.) on March 29, 2006.

PROCEDURAL MATTER

The government moved to amend [(2)] the first line of SOR ¶ 1.b, by deleting the words "You removed a classified IP address," substituting therefore the words, "You removed an IP address, which you believed to be classified." Applicant objected to the amendment. I denied the government's motion because the allegation, as drafted, encompassed the proposed language.

FINDINGS OF FACT

In his answer to the SOR, Applicant denied, with explanations, SOR allegation 1.a. He admitted allegation 1.b. His admissions are incorporated herein as findings of fact. After a thorough review of the pleadings, Applicant's testimony, and the evidence, I make the following additional findings of fact:

Applicant is 29 years old and has never been married. Between 1994 and 1997, he completed approximately two years of college. Applicant has worked in the information technology field since he was approximately 20 years old. For the last nine years, he worked for Department of Defense (DOD) contractors, and held positions such as information systems security manager, system administrator, security engineer, and network and software specialist. Applicant began his training in the handling of classified information in 1996 when he was hired by a government contractor to be their information systems security manager.[(3)] He was required to attend a three-day seminar concerning the handling of classified information. Applicant has held a secret security clearance since 1996-1997.[(4)]

In January 2002, Applicant proposed a scheme to defraud the government to another government contractor employee (X). Applicant and X worked on the same Navy project and shared office facilities. They knew each other through mutual acquaintances, casual conversations at work, and from going out to dinner with mutual friends. While working on the Navy project, X was living in a hotel on a "temporary duty" status. X's employer provided him with a company credit card to pay for his living expenses, including living accommodations, which were then submitted to the government for reimbursement.

Applicant proposed X to enter into a lease for rental property with Applicant's mother (or her property manager) with a rent payment over the value of the actual rent Applicant wanted to be paid. The lease with the inflated rent payment was to be submitted to the government to justify X's rental expenses. The lease with Applicant's mother would conceal the relationship between X and Applicant. X would live in Applicant's house with Applicant, and part of the inflated rent payment made by the government would be applied toward Applicant's mortgage. Applicant would then give the remainder of the inflated rent payment to X, in cash, as a kickback.

One day after the conversation, X reported Applicant's proposal to X's supervisors and government representatives. Applicant's employer confronted Applicant with the allegations, and after Applicant confirmed the basic facts of the allegation, he was terminated from his employment.[(5)] X testified that he considered Applicant's proposal fraudulent and unethical because of the false contract to conceal their relationship, and the kickback, which required billing the government for an inflated rent payment. He felt obligated to disclose the proposal. X's hearing testimony was consistent with an email he sent to his supervisor one day after he disclosed Applicant's proposal to her, and two days after Applicant's proposal.[(6)]

Applicant did not contest his termination or confront X concerning the allegations. Shortly after his termination, Applicant was hired by another government contractor as a software specialist. He has been working for his current employer for approximately 21 months and requires a security clearance to work on government projects.

Applicant explained that X misunderstood his offer to assist him finding less expensive accommodations and to save some money. He testified he did not intend to do anything illegal or to defraud the government. He claimed he believed X was being provided a government per diem rate to compensate X for his living expenses, and that if X used less than his entitlement, X could legally keep the remainder.

In March 2003, Applicant was interviewed by a government investigator. During the interview, Applicant was asked whether he had ever engaged in any security violation. He replied he had not. Applicant disclosed, however, that while troubleshooting a software problem in a computer located in a classified area, he wrote down on a piece of paper the computer's internet protocol address (IP).[(7)] After finishing the repairs, Applicant returned to his office and discovered he still had the piece of paper with the computer's IP address. Applicant admitted he should not have taken the paper out of the classified area. However, he believed the computer IP address was not classified information and he shredded the piece of paper in his office crosscut-shredder. He did not report the incident to the security manager because the information was not classified and he had shredded the paper. Applicant had no intention of taking the piece of paper with him. He testified his action was a careless oversight. There is no record evidence to suggest that a computer's IP address is classified information. To the contrary, according to Applicant's witness' testimony, (one of them works as the chief operating officer for a military service intranet) a computer's IP address is not classified information.[(8)]

At his hearing, Applicant expressed particular pride in his job providing security for government computers and information systems. The testimony of his five witnesses and the letters of recommendation[(9)] attest to his reputation as a responsible, motivated, hardworking, and a valuable employee. Those who are in a position to know him well believe him to be dependable, honest, and trustworthy. His supervisors recognized his superior performance, excellent knowledge and technical skills, and strongly endorsed his suitability for a security clearance.

POLICIES

The Directive sets forth adjudicative guidelines which must be considered in evaluating an Applicant's eligibility for access to classified information. The administrative judge must take into account both disqualifying and mitigating conditions under each adjudicative guideline applicable to the facts and circumstances of the case. The guidelines are not viewed as inflexible ironclad rules of law. The presence or absence of a disqualifying or mitigating condition is not determinative of a conclusion for or against an Applicant. Each decision must also reflect a fair and impartial common sense consideration of the factors listed in Section 6.3 of the Directive, and the whole person concept.[(10)] Having considered the record evidence as a whole, I conclude Guideline E (Personal Conduct) is the applicable relevant adjudicative guideline.

BURDEN OF PROOF

The purpose of a security clearance decision is to determine whether it is clearly consistent with the national interest to grant or continue an applicant's eligibility for access to classified information.[(11)] A person who has access to classified information enters into a fiduciary relationship with the government based on trust and confidence. The government, therefore, has a compelling interest to ensure each applicant possesses the requisite judgment, reliability and trustworthiness of one who will protect the national interests as his or her own.

The government has the initial burden of proving controverted facts alleged in the SOR. To meet its burden, the government must establish, by substantial evidence,[(12)] a prima facie case that it is not clearly consistent with the national interest for the applicant to have access to classified information. The responsibility then shifts to the applicant to refute, extenuate or mitigate the government's case. Because no one has a right to a security clearance, the applicant carries a heavy burden of persuasion.[(13)] The "clearly consistent with the national interest" standard compels resolution of any reasonable doubt about an applicant's suitability for access to classified information in favor of protecting national security.[(14)]

CONCLUSIONS

Under Guideline E, personal conduct is always a security concern because it asks the ultimate question - whether a person's past conduct instills confidence the person can be trusted to properly safeguard classified information. An applicant's conduct is a security concern if it involves questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations. Such behavior could indicate that the person may not properly safeguard classified information.[(15)]

The government established its case under Guideline E by showing that Applicant attempted to defraud the government and/or a government contractor. Applicant's schemed to defraud the government by proposing a false rental property agreement with inflated rent costs. Part of the rent payment would have been applied to Applicant's home mortgage payments, and the remainder was to be given back to X as payment for participating in the scheme - a kickback. Applicant's scheme required premeditation, planning, and the specific intent to defraud.

Applicant vehemently averred that X did not understand that his proposal was to help him save money. He denied any intent to defraud the government because he believed X was on a per diem rate and whatever he had left over after expenses was his money. Considering all available evidence as a whole, Applicant's claims of innocence fall short for several reasons: (X's) testimony was credible and he had no motive to lie either in 2002, when he filed the complaint, or at the hearing; X reported the incident immediately after the conversation and his testimony is corroborated by his contemporary e-mail to one of his supervisors;[16] and Applicant's supervisor's e-mail stating Applicant corroborated the basic facts of the allegations. In light of Applicant's demeanor, testimony, and available evidence, I find Disqualifying Condition (DC) 1: *Reliable, unfavorable information provided by associates, employers, coworkers, neighbors, and other acquaintances*;[17] and DC 4: *Personal conduct or concealment of information that increases an individual's vulnerability to coercion, exploitation or duress such as engaging in activities which, if known, may affect the person's personal, professional, or community standing or render the person susceptible to blackmail*[18] apply.

I considered all Guideline E Mitigating Conditions (MC) and, in light of all the facts and circumstances, I conclude that none applies. I specifically considered whether Applicant's behavior is isolated and/or remote in light of the fact that there is no evidence of any similar behavior before or after the 2002 incident, and Applicant's character reputation. Applicant has impressive character references who respect and hold him in high regard both as a gifted, knowledgeable technician and as a person. They complimented Applicant's integrity, honesty, and truthfulness, endorsed his qualifications for a security clearance, and would welcome Applicant in their companies.

I also considered Applicant's age at the time of the incident, his level of education, the fact he worked for government contractors in government projects for approximately six years, his training in the handling of classified information, and the fact he held important security related jobs as information systems security manager, system administrator, security engineer, and network and software specialist. Applicant knew or should have known his proposal to submit a false rental fee claim was illegal, and his actions were committed with the intent to defraud the government and for his own personal benefit. Applicant's explanations to the contrary are not credible in light of the evidence as a whole.

By holding a security clearance, Applicant entered into a special trust and confidence relationship with the government to protect the nation's secrets. Applicant's attempt to defraud the government violated the trust reposed in him and raised serious questions concerning his honesty, integrity, and judgment. Considering the totality of the circumstances, the nature and seriousness of the behavior, I find that neither Applicant's favorable evidence, nor the passage of time so far, are sufficient to overcome the concerns raised by his egregious behavior. Guideline E is decided against Applicant.

Concerning SOR ¶ 1.b, the record evidence in this case established that a computer's IP address is not classified information. I find the government's argument that Applicant's shredding the paper with the computer IP address shows Applicant believed the information was classified is speculative and not supported by the record evidence. Applicant disclosed the incident during a background interview and clarified that he did not report the incident as a security violation because he believed the computer IP address was not classified. There is no other evidence to establish Applicant's belief at the time he shredded the paper.

I have carefully weighed all evidence, and I applied the disqualifying and mitigating conditions as listed under the applicable adjudicative guideline. Considering all relevant and material facts and circumstances present in this case, including Applicant's testimony, his misconduct, the whole person concept, and the adjudicative factors listed in the Directive, I find Applicant has not mitigated the security concerns.

FORMAL FINDINGS

Formal findings regarding each SOR allegation as required by Directive Section E3.1.25 are as follows:

Paragraph 1, Personal Conduct (Guideline E) AGAINST APPLICANT

Subparagraph 1.a Against Applicant

Subparagraph 1.b For Applicant

DECISION

In light of all the circumstances presented by the record in this case, it is not clearly consistent with the national interest to grant or continue a security clearance for Applicant. Clearance is denied.

Juan J. Rivera

Administrative Judge

1. Required by Executive Order 10865, *Safeguarding Classified Information Within Industry* (Feb. 20, 1960), as amended, and Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (Jan. 2, 1992) (Directive), as amended.

2. The government's motion was made pursuant to DoD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (Directive), Additional Procedural Guidance ¶ E3.1.17.

3. Tr. 126-127.

4. Tr. 71.

5. GE 2.

6. GE 2 and 3.

7. The internet protocol address (IP) is a specific numerical sequence that identifies a particular computer within a network of computers.

8. Tr. 166-167.

9. AE 1 and 2.

10. Directive, ¶ E2.2.1. "The adjudicative process is the careful weighing of a number of variables known as the whole person concept. Available, reliable information about the person, past and present, favorable and unfavorable, should be considered in reaching a determination. . . ."

11. *See Department of the Navy v. Egan*, 484 U.S. 518, 531 (1988).

12. ISCR Case No. 98-0761, at p. 2 (December 27, 1999) (Substantial evidence is more than a scintilla, but less than a preponderance of the evidence.); ISCR Case No. 02-12199, at p. 3 (April 3, 2006) (Substantial evidence is such relevant evidence as a reasonable mind might accept as adequate to support a conclusion in light of all the contrary evidence in the record.); Directive, ¶ E3.1.32.1.

13. *Egan*, 484 U.S. 518, at 528, 531.

14. Directive, ¶ E2.2.2.

15. Directive, ¶ E2.A5.1.1.

16. GE 3.

17. Directive, ¶ E2.A5.1.2.1.

18. Directive, ¶ E2.A5.1.2.4.