KEYWORD: Personal Conduct; Misuse of Information Technology; Criminal Conduct

DIGEST: Applicant is a 46-year-old information security engineer employed by a federal government contractor. He was alleged to have been terminated from employment for inappropriate use of government equipment, visiting inappropriate websites, the loading of unauthorized software on government equipment, and/or deliberately not following instructions and performance issues. He denied the conduct in an interview with the Defense Security Service. The government failed to establish its case about personal conduct, misuse of information technology, and criminal conduct Clearance is granted.

CASENO: 03-23504.h1

DATE: 07/23/2007

DATE: July 23, 2007

	)	
In re:	)	
	)	
----------------------	)	ISCR Case No. 03-23504
SSN: -----------	)	
	)	
Applicant for Security Clearance	)	
	)	

DECISION OF ADMINISTRATIVE JUDGE
CHRISTOPHER GRAHAM

APPEARANCES

FOR GOVERNMENT
James Duffy, Esq., Department Counsel

FOR APPLICANT
Alexander M. Laughlin, Esq.
Rebecca Saitta, Esq.

<u>**SYNOPSIS**</u>

Applicant is a 46-year-old information security engineer employed by a federal government contractor. He was alleged to have been terminated from employment for inappropriate use of government equipment, visiting inappropriate websites, the loading of unauthorized software on government equipment, and/or deliberately not following instructions and performance issues. He denied the conduct in an interview with the Defense Security Service. The government failed to establish its case about personal conduct, misuse of information technology, and criminal conduct Clearance is granted.

STATEMENT OF THE CASE

On May 11, 2005, Applicant submitted a Security Clearance Application (SF 86).[1] The Defense Office of Hearings and Appeals (DOHA) declined to grant or continue a security clearance for Applicant. As required by Executive Order 10865, *Safeguarding Classified Information Within Industry,* dated February 20, 1960, as amended, and Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (Directive), dated January 2, 1992, as amended, DOHA issued a Statement of Reasons (SOR) on January 19, 2005, detailing the basis for its decision – security concerns raised under Guideline E (Personal Conduct), Guideline M (Information Technology Systems), and Guideline J (Criminal Conduct) of the Directive. The President issued revised adjudicative guidelines (Guidelines) on December 30, 2005. DoD implemented them on September 1, 2006. Pending official amendment/reissue of DoD Directive 5220.6, the Guidelines are to be used in all cases when the SOR is dated on or after September 1, 2006. Because the SOR was dated before September 1, 2006, DoD policy requires that this case proceed under the former guidelines.

Applicant answered the SOR in writing on February 18, 2005, and elected to have a hearing before an administrative judge. DOHA assigned the case to me on March 29, 2007, and issued a Notice of Hearing on April 26, 2007. I convened a hearing on May 17, 2007, to consider whether it is clearly consistent with the national interest to grant or continue Applicant's security clearance. The government offered seven exhibits, marked as Exhibits 1-7. I then placed a telephone call to the government's witness. Applicant offered fifteen exhibits, marked as Exhibits A-O. All exhibits were admitted without objection. DOHA received the transcript (Tr.) on May 30, 2007.

FINDINGS OF FACT

Applicant denied all allegations in the SOR. After a complete and thorough review of the evidence in the record, and upon due consideration of same, I make the following findings of fact:

Applicant is a 46-year-old information security engineer employed by a federal government contractor.[2] He is married and has two children.[3] He has an associate college degree.[4] He served in the United States Army for 20 years retiring with the rank of staff sergeant (E-6). He worked with computers, computer programming, and working with soldiers' security clearance applications. He

[1] Government Exhibit 1 (Security Clearance Application (SF 86), dated May 11, 2005).

[2] Tr. at 10, 17.

[3] *Id.* at 11.

[4] *Id.* at 73.

earned Army commendation medals, Army achievement medals, Army Good Conduct medals among numerous awards and citations.[5] He has held a security clearance since 1982.[6]

Applicant worked for a computer software company for about five months in 2002. The government's case was built upon the testimony of the company's program manager. She testified by telephonic conference. The program manager, spent 22 years in the United States Army, military intelligence branch, retiring as a sergeant major in 1998.[7]

The contract that she managed was computer and network security at a military installation. She acted as the interface between the government and the contractor. Applicant's duties were to review the security logs of network monitoring equipment. She stated that some of the rules for government computer use was that you could not load onto your computer any software that had not been approved by the government; you couldn't visit any unauthorized sites, such as pornographic or hacker site; and you were not authorized any personal use on your computer, other than to get e-mails.[8]

The witness alleged that Applicant was reading more of people's e-mails than was necessary to determine if there was a security breach. The system would notify of a potential security violation. Applicant would review the e-mail to see if there were any security issues. If there were none, he was supposed to immediately terminate the connection, back out of it, and not review it anymore. She recalled counseling him because he read an email between a gay person and her mate, which she says he discussed with others in the office. One of the other office members brought it to her attention. She said Applicant basically agreed, apologized and said he wouldn't do it again, and there were no more complaints about it.[9]

She alleged that on another day, Applicant was looking at a website that had women scantily clothed and that it offended a coworker. The first time she gave him a verbal warning and a second time was more formal. She told him what the rules were, that he had signed a statement indicating that he knew the rules when he was hired, and that he was violating the contract with the government. He apologized, said he understood he had done wrong, and wasn't going to do it again.[10]

Next, the witness testified that around September 2002, Applicant had loaded hacker software onto the system that allowed it to track others and access their systems. Another employee was familiar with this software, saw it on Applicant's computer, and reported it to the program manager. Applicant was not authorized to use the software. She counseled him and had some of

[5] *Id.* at 67-70; Applicant's Exhibits D through K.

[6] *Id.* at 74.

[7] *Id.* at 19.

[8] *Id.* at 20-23.

[9] *Id.* at 24-27.

[10] *Id.* at 27-33.

the other computer technicians check out his computer. A week or two later, it occurred a second time. She brought it to the government's attention and was told to immediately remove him from the contract and get him off the site. She told Applicant to log out and shut down his system, and that he needed to gather all his personal items together. When he asked why, he was told that she had again found hacker software on his system. He asked to speak to the government representative in charge, and she told them that the person had specifically told her he didn't want to speak to Applicant. He just wanted him gone.[11]

She also testified that one time, she found Applicant playing solitaire on his computer. Playing games on a government computer was prohibited. However, all games had not been removed from the computers. She said to her knowledge, he never played cards again. She did state she had seen other people playing cards, but she apparently did not warn those people.[12]

She also stated she counseled Applicant on his use of the chain of command. The contractor was having problems with the common intrusion detector director software. She said the government had been made aware of the problems. She said the government liaison complained to her that Applicant had come to him to complain about the system. She wrote him up and explained that she was the interface between the government and the contractor, and that he should direct questions to her. There were problems with the system. It was logging far too many false security intrusion alerts. Genuine security breaches were missed because of the number of false alerts. There was delay in getting program updates.[13]

The employer did not keep a list of appropriate websites, it did not have a list of banned software, she denied instructing Applicant not to advise the government about his candid assessment of the performance of the software. She denied that Applicant was asked directly by the government program manager about the problems with the software. She denied telling Applicant that he must not value his job with the company. She denied that Applicant was asked to leave the company almost immediately after his second discussion with the government manager where he informed him about the continuing deficiencies in the company's product.[14]

Applicant testified his job was to check the alerts that would come up on the console to make sure they were either actual true alerts or if they were false positives. It was his job to protect the system against attempted intrusions for security violations. When the company's software was installed, it had problems in that thousands of false positive alerts were popping up on the console. The government project manager didn't understand why it was taking the company so long to fix it.

Occasionally, the government program manager would stop by Applicant's console and want to know how the program was working. Applicant would show him thousands of alerts and told him the problem is too many alerts, that he could not tell which ones were real and which were false. Applicant said he could go into each alert to examine it, but it was very time consuming and it would

[11] *Id.* at 34-39.

[12] *Id.* at 40-42.

[13] *Id.* at 43-47.

[14] *Id.* at 47-52.

take a lot of man-hours to check each one to verify its authenticity. He asked Applicant if this was normal and Applicant said "No." After the government manager left, the company program manager came to Applicant's desk to ask what the government manager wanted. Applicant told her. She told Applicant that he was not supposed to tell the federal government that anything was wrong with the company's product. Applicant told her that he was asked a question, and it was unethical not to tell them the truth, and the truth was the product was not working like the company had promised. She then told Applicant that she was the program manager for the company and said, "I'll tell him what he needs to know. You don't tell him anything."[15] Applicant told her that she was forcing him into the position where he had to lie, and that he would not lie. She told them to have the government program manager, see her next time.[16] A few days later the government program manager returned, and asked Applicant how the program was working, and Applicant told him that he could not tell him what was going on with the software. At that, the government manager got upset and told Applicant that he (Applicant) would tell him what's going on with the software because he paid Applicant's salary. Being put that way, Applicant told him what was wrong, that the software wasn't reporting correctly, and that too many alerts were popping up on the console. The company program manager then walked over and this exchange followed:

> I overheard you talking to him. What did you tell him? And I said, I told him the truth. And she said, I told you not to talk to him. And I said, hey, I can't lie. I worked for the Army for 20 years. It's against my--it's my--my integrity is on the line. It's unethical. I just won't do it. And she said, well, obviously you don't value your position here. I said, if it means lying, no I don't. And I believe it was a couple days later, when I was asked to pack up my things in a box and depart the area.[17]

Applicant was aware there was a dispute between the government and the contractor about performance. The contract was based on performance and if the time table was not met, the contract could be canceled. Applicant stated that the company did not maintain a list of unauthorized software. Part of his job responsibility was to visit hacker websites. He stated he did not download any unauthorized software. He also did not intercept e-mails. What he did intercept was instant message traffic, which is prohibited by the government. The company did not maintain a list of websites that it deemed appropriate or inappropriate for access by employees. Often when running down a hacking website, other prohibited sites would pop up on the screens. He denied intentionally visiting obscene or inappropriate websites; trying to introduce a virus into the computer system; and illegal entry of the company technologies.

Applicant received a termination letter dated September 23, 2002. The letter does not state the reasons for his termination.[18] The next day, a human resources employee with Applicant's employer wrote herself a memorandum for the record (MFR) stating that Applicant was terminated for inappropriate use of government equipment (visiting inappropriate websites and loading

[15] *Id.* at 86-90.

[16] *Id.* at 90.

[17] *Id.* at 92.

[18] Government Exhibit 3 (Termination Letter, dated September 23, 2002) at 1-2.

unauthorized software on government equipment) and performance issues.[19] About a month later, Applicant's former facility security officer (FSO) sent a letter to Defense Security Services (DSS) informing DSS that Applicant was terminated for inappropriate use of government equipment, visiting inappropriate websites, the loading of unauthorized software on government equipment, to include deliberately not following instructions and performance issues.[20] Applicant denied each of these allegations in a statement to a DSS agent.[21] The SOR alleged that his statement is false, and thereby a criminal act pursuant to 18 U.S.C. § 1001.

In 1996, Applicant was removed from the Army promotion list to sergeant first class (SFC). This occurred because he had demanded that a female soldier participate in physical training (PT) by running with the company, but she had a physical profile which allowed her to run at her own pace.[22]

Applicant's father, uncle, and brother are retired Army officers. His son is in Army training, and his daughter is married to a Marine.[23] His pastor testified about his honesty, character, and integrity.[24] Two co-workers wrote letters of recommendation, describing Applicant's professionalism, trustworthiness, high moral character, and integrity.[25]

POLICIES

In an evaluation of an applicant's security suitability, an administrative judge must consider Enclosure 2 of the Directive, which sets forth adjudicative guidelines. In addition to brief introductory explanations for each guideline, the adjudicative guidelines are divided into Disqualifying Conditions (DC) and Mitigating Conditions (MC), which are used to determine an applicant's eligibility for access to classified information.

These adjudicative guidelines are not inflexible ironclad rules of law. Instead, recognizing the complexities of human behavior, an administrative judge should apply these guidelines in conjunction with the factors listed below. An administrative judge's overarching adjudicative goal is a fair, impartial and common sense decision.

[19] Government Exhibit 4 (Memorandum for the Record, dated September 24, 2002) at 1.

[20] Government Exhibit 2 (Letter to DSS, dated October 18, 2002) at 1.

[21] Government Exhibit 5 (Applicant's Sworn Statement, dated August 11, 2003) at 1-3.

[22] Government Exhibit 6 (Recommendation of Removal from SFC Promotion List, dated November 8, 1996) at 1-4; Government Exhibit 7 (NCO Evaluation Report, dated July 15, 1996) at 1-2.

[23] *Id.* at 103.

[24] *Id.* at 144-150.

[25] Applicant's Exhibits B and C (Letters of Recommendation, dated April 27, 2007) at 1.

Because the entire process is a conscientious scrutiny of a number of variables known as the "whole person concept," an administrative judge should consider all available, reliable information about the person, past and present, favorable and unfavorable, in making a meaningful decision.

Specifically, an administrative judge should consider the nine adjudicative process factors listed at Directive ¶ E2.2.1: (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 voluntariness of participation; (6) the presence or absence of rehabilitation and other pertinent 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.

Since the protection of the national security is the paramount consideration, the final decision in each case is arrived at by applying the standard that the issuance of the clearance is "clearly consistent with the interests 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.

In the decision-making process, facts must be established by "substantial evidence. The government initially has the burden of producing evidence to establish a potentially disqualifying condition under the Directive. Once the government has produced substantial evidence of a disqualifying condition, the burden shifts to the applicant to produce evidence and prove a mitigating condition. [26] Directive ¶ E3.1.15 provides, "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, and [applicant] has the ultimate burden of persuasion as to obtaining a favorable clearance decision." The burden of disproving a mitigating condition never shifts to the government.[27]

A person who seeks access to classified information enters into a fiduciary relationship with the government predicated upon trust and confidence. It is a relationship that transcends normal duty hours and endures throughout off-duty hours as well. It is because of this special relationship the government must be able to repose a high degree of trust and confidence in those individuals to whom it grants access to classified information. Decisions under this Directive include, by necessity, consideration of the possible risk an 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.

[26] "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." ISCR Case No. 04-11463 at 2 (App. Bd. Aug. 4, 2006) (citing Directive ¶ E3.1.32.1). "This is something less than the weight of the evidence, and the possibility of drawing two inconsistent conclusions from the evidence does not prevent [a Judge's] finding from being supported by substantial evidence." *Consolo v. Federal Maritime Comm'n*, 383 U.S. 607, 620 (1966). "Substantial evidence" is "more than a scintilla but less than a preponderance." *See v. Washington Metro. Area Transit Auth.*, 36 F.3d 375, 380 (4th Cir. 1994).

[27] *See* ISCR Case No. 02-31154 at 5 (App. Bd. Sep. 22, 2005). "The Administrative Judge [considers] the record evidence as a whole, both favorable and unfavorable, [evaluates] Applicant's past and current circumstances in light of pertinent provisions of the Directive, and [decides] whether Applicant [has] met his burden of persuasion under Directive ¶ E3.1.15." ISCR Case No. 04-10340 at 2 (App. Bd. July 6, 2006).

The scope of an administrative judge's decision is limited. Applicant's allegiance, loyalty, and patriotism are not at issue in these proceedings. Section 7 of Executive Order 10865 specifically provides industrial security clearance 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." Security clearance decisions cover many characteristics of an applicant other than allegiance, loyalty, and patriotism. Nothing in this Decision should be construed to suggest that I have based this decision, in whole or in part, on any express or implied determination as to Applicant's allegiance, loyalty, or patriotism.

CONCLUSIONS

I conclude that the government failed to establish its case under Guideline E, Guideline M, and Guideline J. Applicant denied the allegations in the SOR. In a controverted case, the government has the burden of establishing its case. The government's case rested upon the testimony of the company program manager. It is apparent that the company had a problem with its software, and the program did not do what it was designed to do. When asked if there was a problem with the software by the government manager, Applicant told the truth and stated that the program had problems and was not working properly. The fact that the company program manager was upset with Applicant for telling the government the truth belies the fact that they expected him to cover up a defective product, and when he refused, retaliated. This finding is reinforced by the fact that she told Applicant that she would tell the government what the government needed to know. In a portion of her testimony, she denied that the government program manager went to Applicant's desk to ask about the software. She also testified that she counseled Applicant for telling the government manager the truth about the software. Her explanation was that Applicant sought out the government manager to bad-mouth the software. We know that Applicant talked to the government manager. I believe his version that he was approached by the government, told the truth, and then was fired.

In looking at the record evidence, none of the after-the-fact exhibits, the MFR nor the letter to DSS show a copy to Applicant. The only letter that Applicant received mentioned no reasons for termination. The government produced no MFR detailing counseling sessions to Applicant, no illegal software, and no documents stating what his performance issues were. The government's case rises or falls on the testimony of Applicant's supervisor. After re-reading the transcript, I did not find her testimony to be credible. My opinion is that Applicant was terminated for telling the government that the software it purchased was defective.

I had the opportunity to evaluate the demeanor of Applicant, observe his manner and deportment, appraise the way in which he responded to questions, assess his candor or evasiveness, read his statements, listen to his testimony, and watch the interplay between himself and those around him. It is my impression Applicant's explanations are both consistent and sincere, and have the solid resonance of truth. Thus, I conclude Applicant has, through evidence of explanation, successfully refuted the Government's case.

FORMAL FINDINGS

Formal findings For or Against Applicant on the allegations set forth in the SOR, as required by E3.1.25 of Enclosure 3 of the Directive, are:

Paragraph 1. Guideline E:	FOR APPLICANT
Subparagraph 1.a:	For Applicant
Subparagraph 1.b:	For Applicant
Paragraph 2. Guideline M:	FOR APPLICANT
Subparagraph 2.a:	For Applicant
Paragraph 3. Guideline J:	FOR APPLICANT
Subparagraph 3.a:	For Applicant

DECISION

In light of all of the circumstances in this case, it is clearly consistent with the national interest to grant or continue a security clearance for Applicant. Clearance is granted.

Christopher Graham
Administrative Judge