

DATE: July 28, 2005

In Re:

SSN: -----

Applicant for Security Clearance

ISCR Case No. 03-07080

DECISION OF ADMINISTRATIVE JUDGE

THOMAS M. CREAN

APPEARANCES

FOR GOVERNMENT

Erin C. Hogan, Esq., Department Counsel

FOR APPLICANT

Pro Se

SYNOPSIS

Applicant is a teleconference specialist for a defense contractor. When employed by a computer service company, Applicant received computer equipment for job training. Applicant did not return the equipment when his employment was terminated. Police seized the equipment from his house. He was charged with theft of property by unauthorized taking and appeared in court, but was informed by the judge to return to court with counsel. Applicant was indicted by grand jury but moved to another state and never returned to court. He pled guilty to the offense later. Applicant failed to list the felony charge on his security clearance application. Applicant denied to a DSS special agent any encounter with law enforcement or knowledge of the felony charges. Applicant has not mitigated security concerns for personal and criminal conduct. Clearance is denied.

STATEMENT OF THE CASE

On September 14, 2004, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) detailing the basis for its decision to deny a security clearance for Applicant. The action was taken under Executive Order 10865, *Safeguarding Classified Information within Industry* (February 20, 1990), as amended and modified, and Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended and modified (Directive). Applicant acknowledged receipt of the SOR on September 23, 2004. The SOR alleges security concerns under Guideline E (Personal Conduct) and Guideline J (Criminal Conduct) of the Directive.

Applicant answered the SOR in writing on October 27, 2004. He admitted three and denied one of the allegations under Guideline E and admitted the three allegations under Guideline J. He requested a hearing before an administrative judge and the request was received by DOHA on October 29, 2004. Department Counsel was prepared to proceed with the case on January 15, 2005, and the case was assigned to another administrative judge on January 18, 2005, and reassigned to me on May 5, 2005. A notice of hearing was issued on May 13, 2005, and the hearing convened on June 7, 2005. Four government exhibits and the testimony of the Applicant were received during the hearing. The transcript was

received on June 28, 2005.

FINDINGS OF FACT

Applicant is a video teleconference specialist for a defense contractor. Applicant was employed by a computer service company as both a sales and customer service representative. He asked for and received computer equipment from his employer to train at home. In December 1995, Applicant's employment was terminated by the computer service company for misconduct relating to Applicant providing perks and incentives to clients beyond instructions from the company. When he was terminated, Applicant did not inform anyone in the company he had the computer equipment and made no attempt to return the equipment. Applicant explained that he forgot about the equipment. He was moving to State A, so he was preoccupied with that move. [\(1\)](#)

Police officers from the local police department came to Applicant's house a few weeks after his termination but before his move to State A. They asked Applicant about computer equipment missing from his former employer and requested permission to search his house. Applicant gave permission explaining he had computer equipment from the company but had no way to return the equipment. After the police seized the equipment, Applicant gave a statement to the police at the police station. Applicant received a complaint notice in late January 1996 to appear in court in March 1996 to answer charges for theft by unauthorized taking of the computer equipment. [\(2\)](#) The court appearance was before Applicant moved to State A, and Applicant appeared in court as ordered. In response to the judge's question concerning counsel, Applicant stated he was not represented by counsel. The judge suggested he obtain counsel and the case was continued. [\(3\)](#)

Applicant tried to obtain counsel from the local public defender but was unsuccessful. He was in the process of moving and called the court clerk to determine if there was a problem with his moving out of state. The clerk told him there was no issue as long as the court had a good contact number for him. Applicant moved to State A in March 1996. After his move to State A, Applicant stated he contacted the clerk of court a number of times and was informed they had no new information on his case. [\(4\)](#)

Applicant was indicted by the grand jury for unlawful taking of the computer equipment on March 19, 1996, and the case was transferred to the trial court on April 1, 1996. Applicant failed to appear at his trial and a warrant was issued for his arrest on April 4, 1996. There is no evidence Applicant received or did not receive notice of the hearing. [\(5\)](#)

Applicant moved from State A in early 2002 to State B, and was employed by his present defense contractor. As part of his new employment, Applicant submitted a security clearance application. [\(6\)](#) Applicant responded "NO" to question 21 asking if he had ever been charged with or convicted of a felony. Applicant was interviewed by a special agent from the Defense Security Service (DSS) in October 2002, and asked about the January 1996 theft of computer equipment charge. Applicant denied having anything to do with stolen or missing computer equipment, and stated he was unaware of the charges. He told the agent he would contact the court to settle the matter. He also denied having any contact with law enforcement officials in the last seven years. [\(7\)](#)

Applicant did contact the court in April 2003, pled guilty to the offense of theft by unauthorized taking as listed in the indictment, and sentenced to 12 months confinement, all but three days suspended, a \$1,000 fine, and two years probation. [\(8\)](#) Applicant was again interviewed by a DSS agent in January 2004, and admitted the actions taken by the court. [\(9\)](#)

POLICIES

The President has "the authority to . . . control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to occupy a position . . . that will give that person access to such information." [\(10\)](#) Eligibility for a security clearance is predicated upon the applicant meeting the security guidelines contained in the Directive. [\(11\)](#)

The Directive sets out the adjudicative guidelines for making decisions on security clearances. Enclosure 2 of the Directive sets forth adjudicative guidelines for determining eligibility for access to classified information, and it lists the disqualifying conditions and mitigating conditions for each guideline. Each clearance decision must be fair, impartial, and a commonsense decision based on the relevant and material facts and circumstances, the whole person concept, and the factors listed in the Directive ¶ 6.3.1 through ¶ 6.3.6.

"The adjudicative process is an examination of a sufficient period of a person's life to make an affirmative determination that the person is eligible for a security clearance." An administrative judge must apply the "whole person concept," and consider and carefully weigh the available, reliable information about the person.⁽¹²⁾ An administrative judge should consider: (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 applicant'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 of recurrence.⁽¹³⁾

A person granted access to classified information enters into a special relationship with the government. 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. The decision to deny an individual a security clearance is not necessarily a determination as to the loyalty of the applicant.⁽¹⁴⁾ It is merely an indication that the applicant has not met the strict guidelines the President and the Secretary of Defense have established for issuing a clearance.

Initially, the Government must present evidence to establish controverted facts in the SOR that disqualify or may disqualify the Applicant from being eligible for access to classified information.⁽¹⁵⁾ Thereafter, Applicant is responsible for presenting evidence to rebut, explain, extenuate, or mitigate facts.⁽¹⁶⁾ An applicant "has the ultimate burden of demonstrating that it is clearly consistent with the national interest to grant or continue his security clearance."⁽¹⁷⁾ "[T]he Directive presumes there is a nexus or rational connection between proven conduct under any of the Criteria listed therein and an applicant's security suitability."⁽¹⁸⁾ "Any doubt as to whether access to classified information is clearly consistent with national security will be resolved in favor of the national security."⁽¹⁹⁾

Based upon a consideration of the evidence, I find the following adjudicative guidelines most pertinent to the evaluation of the facts in this case:

Guideline E - Personal Conduct: A security concern exists for conduct involving questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations. Any of these characteristics in a person could indicate that the person may not properly safeguard classified information.

Guideline J - Criminal Conduct: A security concern exists because a history or pattern of criminal activity creates doubt about a person's judgment, reliability and trustworthiness.

Conditions that could raise a security concern and may be disqualifying, as well as those which would mitigate security concerns, pertaining to the adjudicative guidelines are set forth and discussed in the conclusions section below.

CONCLUSIONS

I carefully considered all of the facts in evidence and the legal standards discussed above. I reach the following conclusions regarding the allegations in the SOR.

The government has established its case under Guideline E. Applicant's taking of computer equipment, false answers on his security clearance application, and false responses to the DSS special agent brings the matter under Personal Conduct Disqualifying Conditions E2.A5.1.2.1 (*reliable, unfavorable information provided by associates, employers, coworkers, neighbors, and other acquaintances*); E2.A5.1.2.2 (*the deliberate omission, concealment, or falsification of relevant and material facts from any personal security questionnaire, personal history statement, or similar form used to conduct investigation . . . determine security clearance eligibility or trustworthiness*); and E2.A5.1.2.3 (*deliberately*

providing false or misleading information concerning relevant and material matters to an investigator, security official, . . . in connection with a security or trustworthiness determination). The employer's report of theft of computer equipment is unfavorable information about Applicant. Question 21 on the security clearance application is straight forward and asks if the applicant has ever been charged with or convicted of a felony. Applicant had appeared in court in response to a felony complaint and informed to obtain counsel. There is no doubt he knew of the felony charges and his answer of "NO" to question 21 is a deliberate omission, concealment or falsification of these charges. Similarly, Applicant knew police officers went to his home in December 1995 to retrieve the computer equipment, he gave a statement to police at the police station, and he subsequently appeared in court for the charge of unauthorized taking of the equipment. His statement to the DSS agent in October 2002 that he was unaware of the charges and had no encounter with law enforcement in the last seven years was a deliberate omission, concealment, or falsification of these facts. He could not forget police officers arriving at his home to retrieve the equipment especially since he subsequently appeared in court to answer the theft charge. The government has established the above disqualifying conditions.

I have considered Personal Conduct Mitigating Conditions E2.A5.1.3.1 (*the information was unsubstantiated or not pertinent to a determination of judgment, trustworthiness, or reliability*); and E2.A5.1.3.2 (*the falsification was an isolated incident, was not recent, and the individual has subsequently provided correct information voluntarily*). Neither mitigating condition pertains to Applicant's case. The charge of theft of computer equipment and Applicant's false statement concerning the incident clearly reflects on Applicant's candor and honesty and are pertinent to a determination of applicant's judgment, trustworthiness, and reliability. The falsifications were not isolated since they were made on both his security clearance application and to the DSS agent. The falsification was recent having been made in conjunction with his security clearance application and the follow-up investigation. While applicant finally admitted the true facts of the incident to a DSS agent on January 14, 2004, he did not do so until confronted by the agent. In this statement, Applicant did not admit to the theft but tried to rationalize it even though he had pled guilty to the offense. His comment to the agent was one of avoidance of responsibility rather than an admission of wrong. I conclude Applicant has not mitigated the security concerns for Personal Conduct.

The government has established its case under Guideline J. Applicant's conviction for theft by unauthorized taking of computer equipment and his false statement on his security clearance application and statement to the DSS agent brings the matter under Criminal Conduct Disqualifying Condition E2.A10.1.2.1 (*allegation or admission of criminal conduct, regardless of whether the person was formally charged*); and E2.A10.1.2.2 (*a single serious crime or multiple lesser offenses*). Applicant pled guilty and was convicted of theft by unauthorized taking. This is both an allegation and an admission of criminal conduct. Applicant also falsified his security clearance application and gave a false statement to the DSS agent. A materially false, fictitious, or fraudulent statement on a security clearance applicant or in a statement to a security agent is a serious federal criminal offense.⁽²⁰⁾ The government has established the above disqualifying conditions.

The Criminal Conduct Mitigating Conditions that may be applicable to Applicant are E2.A10.1.3.1 (*the criminal behavior was not recent*); E2.A10.1.3.2 (*the crime was an isolated incident*); and E2.A10.1.3.6 (*there is clear evidence of successful rehabilitation*). While the actual taking of the computer equipment happened in 1995, Applicant avoided answering for that offense until 2003, thus keeping the incident as recent. Not only did Applicant take the equipment, he twice falsified information so the criminal offenses are linked and not isolated. Applicant has not presented information to show a clear indication of successful rehabilitation from his false statements. In fact, Applicant's taking of the equipment, not mentioning it in answer to an appropriate question, and providing false information to the agent is a clear indication he is not rehabilitated. I conclude Applicant has not mitigated the security concerns for criminal conduct.

I carefully considered all of the circumstances in light of the "whole person" concept. I conclude Applicant is not eligible for access to classified information.

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 E: AGAINST APPLICANT

Subparagraph 1.a.: Against Applicant

Subparagraph 1.b.: Against Applicant

Subparagraph 1.c.: Against Applicant

Subparagraph 1.d.: Against Applicant

Paragraph 2, Guideline J: AGAINST APPLICANT

Subparagraph 2.a.: Against Applicant

Subparagraph 2.b. Against Applicant

DECISION

In light of all of the circumstances in 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.

Thomas M. Crean

Administrative Judge

1. Tr. 15-18.
2. Government exhibit 4 (Court Documents, Complaint, dated Jan. 29, 1996).
3. Tr. 19-22.
4. Tr. 24-26.
5. Government exhibit 1 (Court documents, Attachment 2, Grand Jury true bill, dated Mar. 19, 1996, and arrest warrant, dated Apr. 4, 1996).
6. Government exhibit 1 (Security clearance application, dated Mar. 6, 2002).
7. Government exhibit 2 (Applicant's statement, dated Oct. 29, 2002).
8. Government exhibit 4 (Court documents, Court findings and sentence, dated Apr. 17, 2003).
9. Government exhibit 3 (Applicant's statement, dated Jan. 14, 2004).
10. *Department of the Navy v. Egan*, 484 U.S. 518 (1988).
11. Directive ¶ E2.2.1.
12. *Id.*
13. Directive ¶¶ E2.2.1.1 through E2.2.1.9.
14. *See* Exec. Or. 10865 § 7.
15. Directive ¶ E3.1.14.
16. ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002); *see* Directive ¶ E3.1.15.

17. ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002).
18. ISCR Case No. 95-0611 at 2 (App. Bd. May 2, 1996) (quoting DISCR Case No. 92-1106 (App. Bd. Oct. 7, 1993))
19. *Egan*, 484 U.S. at 531; *see* Directive ¶ E2.2.2.
20. 18 U.S.C. ¶ 1001(a).