DATE: January 31, 2007

In re:

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

Applicant for Security Clearance

ISCR Case No. 03-20453

ECISION OF ADMINISTRATIVE JUDGE

MARY E. HENRY

APPEARANCES

FOR GOVERNMENT

Daniel F. Crowley, Esq., Department Counsel

FOR APPLICANT

Pro Se

SYNOPSIS

Applicant accessed a United States Army computer system using his personal knowledge of the system and generic passwords, not with an authorized password, in violation of federal law and the government warning about use of its computer systems. He accessed the system to obtain data related to contract work to be performed by his employer on behalf of the United States Army, not for personal gain. He has mitigated the government's concerns regarding his person conduct, criminal conduct and misuse of information technology systems. Clearance is granted.

STATEMENT OF THE CASE

On July 14, 2004 , the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) to Applicant, pursuant to Executive Order 10865, *Safeguarding Classified Information Within Industry*, dated February 20, 1960, as amended, and Department of Defense Directive 5220.6, *Defense Industrial Security Clearance Review Program* (Directive), dated January 2, 1992, as amended. The SOR detailed reasons why DOHA could not make the preliminary affirmative finding under the Directive that it is clearly consistent with the national interest to grant or continue a security clearance for Applicant. Specifically, the SOR set forth security concerns arising under Guidelines M (Misuse of Information Technology Systems), J (Criminal Conduct) and E (Personal Conduct) of the Directive. DOHA recommended the case be referred to an administrative judge to determine whether a clearance should be granted, continued, denied, or revoked. On September 1, 2004, Applicant submitted a notarized response to the allegations. He requested a hearing.

This matter was assigned to me on December 18, 2006. DOHA issued A Notice of Hearing on December 20, 2006, and I held a hearing on January 12, 2007. Four government exhibits, submitted and marked as Government Exhibits 1 through 4, were admitted into evidence.[(1)] Applicant did not submit any additional evidence. The government investigator and Applicant testified. The hearing transcript was received on January 23, 2007.

FINDINGS OF FACT

Applicant admitted the allegations under Guideline M, subparagraph1.a. and Guideline J, Subparagraph 2.a. of the SOR. Those admissions are incorporated as findings of fact. He denied the remaining allegations.[(2)] After a complete review of the evidence in the record and upon due consideration, I make the following findings of fact.

Applicant is 56 years old and President and Chief Executive Officer of a defense contractor company. He has held this position for more than six years. Prior to developing his own business, he worked almost three years for defense contractors. He served 29 years in the United States Army and retired as a Chief Warrant Officer (CW4) in 1997. He completed a security clearance application (SF 86) in November 2001.[(3)]

During his military career, Applicant became an expert in logistics automated systems. Upon his retirement from the military and based on his expertise, a defense contractor hired him as a senior project manager. His employer had successfully obtained a contract from the United States Army to analyze its computer data on filling and completing requisitions for repair parts for Army equipment. Under the contract, his employer had access to the Army computer systems to pull unclassified data, analyze it and deliver results of the analysis. His employer established a computer lab and set up a specific computer to receive unclassified data from the Army's computer systems. The contract also provided that his employer would have a user account and password to access the system.[(4)] The contract is not in evidence.

Applicant did not receive training from his employer on security procedures at its company or under the contract. His company rules are not part of the record. When he was hired, he learned that co-workers used anonymous or guest accounts and generic passwords to access government computers to perform work assignments. Since he had just retired from his position with the Army, he had knowledge about eight passwords which would allow him access to the Army's relevant computer systems through the use of anonymous or guest accounts. Although his employer had applied for an authorized password and user account, it had not been received by March 1998. Because he needed to begin his work in order to meet the contract deadlines and he desired to work efficiently and quickly, on numerous occasions in 1998, Applicant, from his office computer, accessed the Army's computer systems through the use of anonymous or guest accounts and generic passwords known to him, and transferred copies of Army computer files relevant to his employer's data analysis work to the office computer lab.[(5)] At a later point in time, his employer received its user account and password information.[(6)]

On March 25, 1998 and again on May 11, 1998, the Army's computer intrusion sensors indicated that a probable computer intrusion had occurred.[(7)] The Army Computer Emergency Response Team (ACERT) notified the Army's Criminal Investigation Division (CID) of the probable intrusion on April 8, 1998 and again in May 1998. A CID special agent trained in fraud and computer crimes began an investigation into the intrusions. He concluded that an intrusion to the Army's computer system had occurred and files had been transferred, which he said meant copied. The investigator determined that the intrusion was semi-normal because the intruder had knowledge about the system. However, the lack of an authorized password made the intrusion not normal. Based on his review of the computer logs, the investigator found an internet protocol (IP) address, which lead him to an Internet Service Provider (ISP), in this case AOL.[(8)]

The investigator obtained a search warrant for AOL's computer logs. From these logs, the investigator determined that the IP address shown on the Army's computer logs belonged to Applicant. The investigator also determined that activity on Applicant's AOL account matched the

dates and times of the intrusion. The investigator then obtained a search warrant for Applicant's home and place of work. Pursuant to the warrant, his staff seized a desktop computer, a laptop computer, several boxes of software and several boxes of computer discs from Applicant's home. The investigator and his staff carefully reviewed all this equipment, plus Applicant's office desktop computer and one more office computer. They found no government files on any of this equipment, software or discs. They did not search the computers in his employer's computer lab, as they were not aware that his employer had a computer lab with the capability to access government computers, including the Army computer systems.[(9)]

The investigator testified at the hearing. He admitted that he had no knowledge as to where the Army's files had been

transferred. He could not describe the contents of the files transferred as he had never reviewed the files. He acknowledged that the files and computer systems did not contain sensitive or classified information, that the files had not been compromised by the intrusion, that the Army's computer systems had not been harmed by the intrusion, and that the security procedures and practices were lax at this time. He never interviewed Applicant nor did he talk with co-workers about the office practice of using generic password and guest accounts to access government computers. His employer stated that it did not condone this practice.[(10)]

The Army contacted the United States Attorney (US Attorney) about prosecution of this case under 18 U.S.C. § 1030(a)(2)(B). This section of the Code outlines numerous circumstances when access to computers could constitute fraud. Section(a)(2)(B), when read as a whole, provides "Whoever … intentionally accesses a computer without authorization or exceeds authorization access, and thereby obtains … information from any department or agency of the United States …" as a basis for possible criminal conduct. 18 U.S.C. § 1030(e)(6) defines the term exceeds authorization as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." While it is beyond the scope of this decision to decide if Applicant violated the statute, it is clear that the under the facts of this case, the US Attorney decided not to seek an indictment and proceed with prosecution. The issue of whether Applicant actually accessed the Army's computer without authorization because he did not have a specific password, even though the Army contract authorized access to the Army's computer systems, would be for a jury to decide. The statutory provisions do not clearly address a situation such as this case.

Based on the initial information provided by the investigator, the US Attorney mailed Applicant a letter advising that he was under investigation for computer fraud. Applicant retained counsel. In February 1999 with his counsel, he met with the US Attorney, the investigator and an FBI agent. At this meeting, Applicant admitted he accessed a government computer without an authorized password. He agreed to a pretrial diversion program. As a result of the meeting, the US Attorney did not proceed forward with this case and the Army discontinued its investigation. Applicant was never arrested, charged or indicted, or convicted of any crime related to his intrusion.[(11)]

During his many years of military service, Applicant held a clearance. In order to obtain work for his business, he completed an SF-86 in November 2001. He answered "no" to the following question:[(12)]

Question 26. Your police Record - Other Offenses

In the last 7 years, have you been arrested for, charged with, or convicted of any offense(s) not listed in modules 21, 22, 23, 24, or 25? (Leave out traffic fines of less than $150 unless the violation was alcohol or drug related.) For this item, report information regardless of whether the record in your case has been 'sealed' or otherwise stricken from the court record. The single exception to this requirement is for certain convictions under the Federal Controlled Substances Act for which the court issued an expungement order under the authority of 21 U.S.C. 844 or 18 U.S.C. 3607.

When Applicant met with the US Attorney, he acknowledged the intrusion, and some months later, signed a Pretrial Diversion Agreement. The top of the agreement identifies this matter as "In the United States District Court for the Eastern District of (state), (City) Division", and is captioned United States of America v. Applicant's name. The document contains no identifying court case number, which would show that this case is part of an official court record.[(13)] If Applicant complied with the terms of the agreement, which he did, the US Attorney would not proceed with prosecution of a case against Applicant. The record contains no documents related to an arrest or indictment of Applicant. Applicant testified that he had been advised by his counsel and the US Attorney that no record of the investigation would exist if he complied with the terms of the Pretrial Diversion Agreement. Based on this representation and his knowledge that he had never been arrested for a crime, he answered no.[(14)]

Applicant's intrusion caused no harm to the Army's computer system by deleting files, introducing viruses, or other such malicious activity. He had no personal need for the data, and he did not gain any personal benefit from his actions. He acknowledges that he saw the initial warning about the a person's right to use government computers, but paid little attention because he had seen it may times.[(15)] Prior to the events of September 11, 2001, security throughout the chain of command in the Army was lax in terms of the use of generic passwords and guest accounts. The Army had developed a system of guest or anonymous accounts and generic passwords to enable to soldiers and contractors in the field to

exchange data more easily. In 1998, most computers "deployed from software"[(16)] had an anonymous account, meaning no user name required. This allowed any name to be placed in an account and a password to be entered. Since September 11, 2001, the security procedures for access to computers have changed and tightened significantly.[(17)]

After the 1998 intrusion, Applicant has not accessed a government computer without the requisite password. His work involves contracts with the government. No additional problems have been shown to have occurred regarding his access to computers.[(18)]

POLICIES

Enclosure 2 of the Directive sets forth adjudicative guidelines which must be considered in the evaluation of security suitability. An administrative judge need not view the adjudicative guidelines as inflexible ironclad rules of law. Instead, acknowledging the complexities of human behavior, these guidelines, when applied in conjunction with the factors set forth in the adjudicative process provision in Paragraph E2.2., Enclosure 2 of the Directive, are intended to assist the administrative judge in reaching fair and impartial common sense decisions.

Included in the guidelines are disqualifying conditions and mitigating conditions applicable to each specific guideline. Although the presence or absence of a particular condition or factor for or against clearance is not outcome determinative, the adjudicative guidelines should be followed whenever a case can be measured against this policy guidance. In addition, each security clearance decision must be based on the relevant and material facts and circumstances, the whole-person concept, and the factors listed in the Directive. Specifically, these are: (1) the nature, extent, and seriousness of the conduct; (2) the circumstances surrounding the conduct; (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 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.[(19)]

The sole purpose of a security clearance determination is to decide if it is clearly consistent with the national interest to grant or continue a security clearance for an applicant.[(20)] The government has the burden of proving controverted facts.[(21)] The burden of proof is something less than a preponderance of the evidence.[(22)] Once the government has met its burden, the burden shifts to the applicant to present evidence of refutation, extenuation, or mitigation to overcome the case against him.[(23)] Additionally, an applicant has the ultimate burden of persuasion to obtain a favorable clearance decision.[(24)]

No one has a right to a security clearance,[(25)] and "the clearly consistent standard indicates that security clearance determinations should err, if they must, on the side of denials."[(26)] Any reasonable doubt about whether an applicant should be allowed access to sensitive information must be resolved in favor of protecting such sensitive information.[(27)] 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." The decision to deny an individual a security clearance is not necessarily a determination as to the allegiance, loyalty, and patriotism of an applicant.[(28)] 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.

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

Misuse of Information Technology Systems - Guideline M: Noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual's trustworthiness, willingness, and ability to properly protect classified systems, networks, and information. Information Technology Systems include all related equipment used for the communication, transmission, processing, manipulation, and storage of classified or sensitive information.

Criminal Conduct - Guideline J: A history or pattern of criminal activity creates doubt about a person's

judgment, reliability and trustworthiness.

Personal Conduct - Guideline E: Conduct involving questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulation could indicate that the person may not properly safeguard classified information.

CONCLUSIONS

Upon consideration of all the facts in evidence, and after application of all appropriate adjudicative factors, I conclude the following with respect to the allegations set forth in the SOR:

Guideline M - Misuse of Information Technology Systems

The government has establish a *prima facie* case under Guideline M. Misuse of Information Technology Systems Disqualifying Condition E2.13.1.2.1. (*illegal or unauthorized entry into any information technology system*) applies. Prior to being issued an user account and password, Applicant accessed the Army's computer system and downloaded files to a computer in his office computer lab. Because he did not have an approved password, his actions constitutes unauthorized entry into a government information technology system.

I have considered the Misuse of Information Technology Systems (MI MC) and conclude that MI MC E2.A13.1.3.1. (*The misuse was not recent or significant*) applies. Applicant's unauthorized use of the Army's computer system occurred more than eight years ago. He accessed the Army's computer system for the sole purpose of retrieving data needed to perform the work required under his employer's contract with the Army. He downloaded relevant data files to a computer in his office, which his employer had designated for receiving government data files. His co-workers regularly used anonymous or guest accounts and generic passwords to access government computer. As a recent Army retiree, he knew the system in question and the passwords which would allow him access without an assigned password, like his co-workers. His repeated intrusions during a specific period of time sought only to gain access to files necessary to complete his work under the Army's contract, not for personal gain or benefit. His intrusions did not harm or change the government computer system. He never manipulated the system for his own advantage or a competitive advantage for his employer. His actions constitute a technical violation of this Guideline, but do not rise to the level of a security concern, making his misuse is not significant.

MI MC E2.A13.1.3.4. (*The misuse was an isolated event*) has some applicability in that Applicant's intrusions occurred during a specific time frame in 1998 and were done solely to obtain data necessary to perform duties under a contract with the Army. Likewise, MI MC E13.A1.3.5. (*The misuse was followed by a prompt, good faith effort to correct the situation*) has partial application. Applicant stopped using the guest accounts and generic passwords once he obtained an authorized password. Since the events of 1998, he has never accessed a government computer without an authorized password.

Guideline J - Criminal Conduct

The government has established its case under Guideline J. Criminal Conduct Disqualifying Condition E2.A10.1.2.1. (*Allegation or admission of criminal misconduct, regardless of whether the person was formally charged*) applies based on Applicant's acknowledgment that he received a letter from the US Attorney informing him that he was being investigated for possible computer fraud, and the Army CID's investigation of him for an intrusion into the Army's computer systems without an authorized password as a violation of federal law.

Initially, I find that the evidence of record is insufficient to establish that Applicant has been arrested, charged or indicted for any crime related to the computer fraud investigation. Although Applicant admitted this allegation, his credible hearing testimony negated his admission that he had been charged with computer fraud. Given that a concern has been raised by the allegation of computer fraud, I considered all the Criminal Conduct Mitigating Conditions (CC MC). I conclude that CC MC E2.A10.1.3.1. (*The criminal behavior was not recent*); and CC MC E2.A10.1.3.6. (*There is clear evidence of successful rehabilitation*) apply. The allegation of computer fraud occurred almost nine years ago. There is no other indication of similar conduct after his actions in 1998. Applicant has not attempted to access a government computer without the requisite password in performing his current contract work. Although he was part of a

criminal investigation for this intrusion, he has never been arrested, charged or convicted of any crimes. He continues to comply with the law, rules and regulations.

Guideline E - Personal Conduct

Under Guideline E, the government must establish that Applicant omitted material facts from his SF-86, and that the omission was deliberate and intentional. I find that the evidence is insufficient to establish that Applicant omitted a material fact when he answered "no" to Question 26. Question 26 asks if Applicant has been **arrested, charged or convicted** of a crime in the last seven years. The record contains no police report, indictment or other criminal charging document, stemming from the US Attorney's and Army's investigation of this incident. Although the Army, in conjunction with the US Attorney, investigated Applicant for possible computer fraud, he was never arrested, charged or convicted of any crime as a result of his intrusion into the Army's computer system in April and May 1998.[(29)] The fact that he went into the pretrial diversion program does not support the government's case. He entered this program prior to an indictment or arrest after reaching an early agreement with the US Attorney, which ended any further investigation and precluded the filing of criminal charges (indictment). The diversion agreement contains no court case number, which is needed to locate all court cases and is a clear indication that no court proceedings were ever instituted in this case.

Regarding the allegation that Applicant's conduct in this matter reflects a pattern of dishonesty or rules violation and could make him vulnerable to coercion, exploitation or duress, the government has established a *prima facie* case. Personal Conduct Disqualifying Condition (PC DC) E2.A5.1.2.4. (*Personal conduct...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*) and PC DC E2.A5.1.2.5. (*A pattern of dishonesty or rule violations, including violation of any written or recorded agreement between the individual and the agency*) apply. Between March and at least May 1998, Applicant repeatedly accessed the Army's computer system with a generic password and transferred computer files to a designed office computer in violation of the reservation of government rights warning given each and every time he accessed the computer.

I have considered the Personal Conduct Mitigating Conditions (PC MC), and conclude that PC MC E2.A5.1.3.5. (*The individual has taken positive steps to significantly reduce or eliminate vulnerability to coercion, exploitation, or duress*) applies. Applicant's intrusions to the Army's computer stopped when he received an authorized password. Subsequent to 1998 and in light of the criminal investigation, Applicant has not attempted to access any government computers without the appropriate authorization. Since this specific period of time in 1998, he has complied with the rules regarding usage of a government computer, and continues to do so, as a contractor for the government with access to government computer systems. No additional evidence of noncompliance with government right to use rules regarding computer usage has been presented.

Whole Person Analysis

Protection of our national security is of paramount concern. Security clearance decisions are not intended to assign guilt or to impose further punishment for past transgressions. Rather, the objective of the adjudicative process is the fair-minded, commonsense assessment of a person's trustworthiness and fitness for access to classified information. Thus, in reaching this decision, I have considered the whole person concept in evaluating Appellant's risk and vulnerability in protecting our national interests.

Applicant served in the Army for 29 years. Through hard work, he rose to the rank of Chief Warrant Officer (CW4), based on a stellar performance. He developed technical expertise in military computer systems, a skill which enabled him to obtain employment after his retirement and led to his decision to use his knowledge to access the Army's computer system in a manner used by his co-workers and without an authorized password. He intended to, and did, obtain only that information necessary to do his job under his employer's government contract. He neither sought nor obtained any personal benefit from his actions, nor did he in anyway harm the Army's computer systems. For a period of months, his access without an authorized password occurred regularly, but ceased when he received the appropriate access account and password. He never manipulated the Army's computer system for any nefarious purpose or for any reason.

Applicant has taken responsibility for his conduct. He completed the requirements of the Pretrial Diversion Program. He currently owns and operates his own business, which performs government contract work. He has never been involved in any other criminal conduct, and is unlikely to engage in this conduct in the future. His long and stellar career with the Army, his stable finances, secure lifestyle, and lack of a criminal record reflect an individual who can be trusted to protect the government's classified information. He made a incorrect decision to use a generic password to access the Army's computer system, which led to a technical violation of Guideline M. He has learned from this mistake and is not likely to repeat it in the future. He is not likely to succumb to pressure, coercion, exploitation or duress for this conduct. Although his employer said it did not condone his activity, it was common practice in the workplace to access government computers in the method used by Applicant. Although his conduct was inappropriate, his actions reflect no intent to violate the rules. Under these circumstances, his conduct noes not rise to the level of a security concern. Accordingly, for the reasons stated, I find that Applicant has mitigated the government's security concerns, and that it is clearly consistent with the national interest to grant a security clearance to Applicant.

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:

SOR ¶ 1-Guideline M : FOR APPLICANT

Subparagraph a-b: For Applicant

SOR ¶ 2-Guideline J: FOR APPLICANT

Subparagraph a For Applicant

SOR ¶ 3-Guideline E: FOR APPLICANT

Subparagraph a-b: For Applicant

DECISION

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

Mary E. Henry

Administrative Judge

1. Government Exhibit 3 had been classified as secret. However, the government provided evidence that this document has been properly declassified, making it proper evidence for submission. Government Exhibit 3 (Record of United States Army Criminal Investigation Command) at 2.

2. Applicant's response to the SOR, dated September 1, 2004, at 4.

3. Government Exhibit 1 (Applicant's security clearance application, dated November 5, 2001) at 1-3, 7.

4. Tr. at 82-84.

5. Applicant did not access these files to gain a business edge over a competitor.

6. Tr. at 84-86, 93-95, 102.

7. Sensors are activated after the intruder fails two or more times to access the computer system, then succeeds in accessing the computer. Tr. at 50.

8. Tr. at 21-36; Government Exhibit 3, *supra* note 1, at Exhibit 4.

9. Tr. at 36-41, 58-59, 66-67; Government Exhibit 3, *supra* note 1, at Exhibits 7-11.

10. Tr. at 43, 47, 58-60, 63, 65.

11. Tr. at 87-93; Government Exhibit 3, *supra* note 1, contains no documents reflecting an arrest or charge against Applicant.

12. Government Exhibit 1, *supra* note 3, at 1, 10-11.

13. Government Exhibit 4 (Pretrial Diversion Agreement, dated September and October 1999) at 1. The two search warrants in the record have different court case numbers. Any court action against the Applicant would required a new court case number. Government Exhibit 3, *supra* note 1, Exhibits 7 and 8.

14. Tr. at 79-80, 99-101.

15. The record does not contain any other evidence of a violation of other government rules.

16. The investigator used this term, which he did not clarify. Tr. at 48-49.

17. Tr. at 47-50, 53, 78, 83.

18. Government Exhibit 1, *supra* note 3, at 2.

19. Directive, Enclosure 2, ¶ E2.2.1.1. through E2.2.1.9.

20. ISCR Case No. 96-0277 at 2 (App. Bd., July 11, 1997).

21. ISCR Case No. 97-0016 at 3 (App. Bd., December 31, 1997); Directive, Enclosure 3, ¶ E3.1.14.

22. *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988).

23. ISCR Case No. 94-1075 at 3-4 (App. Bd., August 10, 1995); Directive, Enclosure 3, ¶ E3.1.15.

24. ISCR Case No. 93-1390 at 7-8 (App. Bd. Decision and Reversal Order, January 27, 1995); Directive, Enclosure 3, ¶ E3.1.15.

25. *Egan*, 484 U.S. at 531.

26. *Id*.

27. *Id*.; Directive, Enclosure 2, ¶ E2.2.2.

28. Executive Order No. 10865 § 7.

29. An investigation is an inquiry into the facts surrounding the intrusion to determine if there is sufficient evidence of a crime. In criminal law, a charge is an accusation that an individual committed a specific crime.