DATE: December 11, 2006

In re:

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

Applicant for Security Clearance

CR Case No. 04-08749

DECISION OF ADMINISTRATIVE JUDGE

CAROL G. RICCIARDELLO

APPEARANCES

FOR GOVERNMENT

Eric Borgstrom, Esq., Department Counsel

FOR APPLICANT

Thomas Albin, Esq.

SYNOPSIS

Applicant is 51 years old and is a senior illustration designer who has worked for the same federal contractor for 30 years. While working in a space with classified computers, he misused company equipment by making copies of music CDs and viewed and edited personal photographs on a classified computer. Applicant's record is otherwise unblemished. He has successfully mitigated security concerns raised under Guideline M, misuse of information technology systems, Guideline E, personal conduct, and Guideline K, security violations. Clearance is granted.

STATEMENT OF THE CASE

The Defense Office of Hearings and Appeals (DOHA) declined to grant or continue a security clearance for Applicant. On July 5, 2005, under the applicable Executive Order[(1)] and Department of Defense Directive,[(2)] DOHA issued a Statement of Reasons (SOR), detailing the basis for its decision-security concerns raised under Guideline M, (Misuse of Information Technology Systems), Guideline E (Personal Conduct), and Guideline K (Security Violations) of the Directive. Applicant answered the SOR in writing on July 19, 2005, and elected to have a hearing before an administrative judge. In his Answer, Applicant admitted all of the allegations under Guidelines M, and denied the portions of allegations under Guidelines E and K. The case was assigned to another administrative judge on June 27, 2006, and reassigned to me on October 2, 2006. A notice of hearing was issued on October 13, 2006, scheduling the hearing for November 1, 2006. I conducted the hearing as scheduled to consider whether it is clearly consistent with the national interest to grant or continue a security clearance. The Government offered eighteen exhibits for admission in the record and were marked as Government Exhibits (GE) 1-18. The exhibits were admitted into evidence without objection. Applicant testified on his own behalf, called four witnesses, and offered six exhibits for admission in to the record. They were marked as Applicant's Exhibits A-F and were admitted into evidence without objection. DOHA received the hearing transcript (Tr.) on November 16, 2006.

FINDINGS OF FACT

Applicant's admissions to the allegations in the SOR, are incorporated herein. In addition, after a thorough and careful

review of the pleadings, exhibits, and testimony, I make the following findings of fact:

Applicant is 51 years old and began working for a federal contractor in 1974. He was laid off in 1977 and returned to work with the same employer in 1979. He continued his work until April 2003, when he was terminated due to violation of company rules and regulations. He appealed his termination and received an 82 day suspension without pay and was permitted to return to work with the stipulation that any further violations would result in immediate termination. He was reinstated in June 2003, and continues to work as a senior illustration designer. He has been married for 17 years and has one child.

Applicant admitted that during the period from approximately 1997 to March 2003, he used company equipment to duplicate compact disks (CDs) and make labels for the CDs for his personal use, and also the use of some coworkers and his supervisor. He admitted that prior to March 2003, he introduced digitized photographs onto his company's classified computer so he could view and edit them for both himself and coworkers. He also concurred that his actions were in violation of company rules, procedures and guidelines, and in some cases in violation of DoD 5220.22-M, the National Industrial Security Program Operating Manual (NISPOM). Applicant also admitted that he took for his personal use discarded plastic sleeves that previously protected company CDs. When the CDs became corrupted they were destroyed, and the plastic sleeves were discarded in the trash.

Applicant worked in a secure area with approximately 20-30 coworkers. Computers were his hobby and he was familiar with how to use certain computer software and hardware. The area where he worked had a CD duplicator that was a stand alone appliance. It also had a label-maker that was hooked up much like a computer printer and could be used by office personnel. From 1997 to 2003 he copied personal music CDs for himself and others in the office at their request. He regularly made copies for his supervisor at his request. From the witnesses' testimony and the evidence presented, it was obvious that others either copied CDs for personal use or had Applicant do it for them. However, once Applicant was disciplined no one wanted to admit they too were involved. There was obvious evasiveness and selective memory in their testimony. I find it was a common practice among the office personnel to copy or have copied CDs for personal use. In October 2001, Applicant obtained his own personal CD duplicator and no longer used the company's equipment for his personal use, but he did use it to copy CDs when requested by his supervisor and other coworkers. I find the reason he did this was because he was assisting his coworkers and supervisors who were less computer savvy then he was.

The photos that Applicant viewed and edited were for himself, his coworkers and his supervisor. The types of photographs were of a personal nature, such as those from the company Christmas party, family photos, and photos used for retirement purposes. Applicant did these things during the work day, but would make up the time if it impacted his workload. He did not believe he was loading software on the computer that remained on the drive, but believed the software was held in a temporary file that was used for viewing and was immediately deleted after he completed viewing and editing the material. It is unclear what type of software was loaded or not and what the ramifications were for corrupting the computer or potentially jeopardizing classified material. However, it is clear Applicant was not authorized to introduce anything on his classified computer.

Applicant and his coworkers received security briefings. However, I find these briefings were perfunctory, at best. Although in many cases it might involve a briefing sheet, there was very little oversight over the briefings and in some cases it consisted merely of handing a piece of paper to an employee and telling them when they got a chance to read it and sign the sheet. Applicant was responsible for abiding by all of the security rules and procedures, but I find the level of ensuring people knew what the rules were and having them reinforced annually was lax.

At the time Applicant was making copies of CDs and using the label maker, I find he was not aware that his actions were a violation of security rules. Some time prior to being disciplined his supervisor told him he should limit his personal use of the equipment and he complied. However, his supervisor also continued to have Applicant make personal copies for him.

Applicant took transparent plastic CD sleeve holders that had previously belonged to his company, for his personal use. These sleeve holders had been discarded in the trash when he obtained them. There were no distinguishable markings on them. It was reasonable for Applicant to assume that once discarded in the trash that the company no longer needed or

wanted them and he was permitted to take them for his personal use.

Applicant is considered by his friends, coworkers and supervisors to be a trustworthy person. He belongs to a yacht club where he is responsible for running the store associated with it. He has a fiduciary responsibility and a financial obligation that he has maintained during his tenure there with no discrepancies. Applicant has never been in trouble with his company in the past 30 years, and since being reinstated has had no further disciplinary issues.[(3)] In 2002, Applicant received a recognition award for being the top performer of the illustration group and had worked the most hours of anyone in the group. He worked extra hours to get the job done and on average was 30% under job estimates. He was considered a valuable asset to the group and department.[(4)] Applicant has maintained his security clearance since he was reinstated and has a renewed sense of commitment to security rules and regulations.

POLICIES

Enclosure 2 of the Directive sets forth adjudicative guidelines to be considered in evaluating a person's eligibility to hold a security clearance. Included in the guidelines are disqualifying conditions (DC) and mitigating conditions (MC) applicable to each specific guideline. Additionally, each security clearance decision must be a fair and impartial commonsense decision based on the relevant and material facts and circumstances, the whole-person concept, along with the factors listed in the Directive. Specifically these are: (1) the nature and seriousness of the conduct and surrounding circumstances; (2) the frequency and recency of the conduct; (3) the age of the applicant; (4) the motivation of the applicant, and the extent to which the conduct was negligent, willful, voluntary, or undertaken with knowledge of the consequences; (5) the absence or presence of rehabilitation; and (6) the probability that the circumstances or conduct will continue or recur in the future. 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.

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.[(5)] The government has the burden of proving controverted facts.[(6)] The burden of proof is something less than a preponderance of evidence.[(7)] Once the government has met its burden, the burden shifts to an applicant to present evidence of refutation, extenuation, or mitigation to overcome the case against him.[(8)] Additionally, an applicant has the ultimate burden of persuasion to obtain a favorable clearance decision.[(9)]

No one has a right to a security clearance[(10)] and "the clearly consistent standard indicates that security clearance determinations should err, if they must, on the side of denials."[(11)] Any reasonable doubt about whether an applicant should be allowed access to sensitive information must be resolved in favor of protecting such sensitive information.[(12)] The decision to deny an individual a security clearance is not necessarily a determination as to the loyalty of an applicant.[(13)] 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 consideration of the evidence, I find the following adjudicative guidelines most pertinent to the evaluation of the facts in this case:

Misuse of Information Technology Systems-is a security concern because 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.

Personal Conduct-is security concern because conduct involving questionable judgment, untrustworthiness, unreliability, lack of candor, dishonest, or unwillingness to comply with rules and regulations could indicate that the person may not properly safeguard classified information.

Security Violations-are a security concern because noncompliance with security regulations raises doubt about an

individual's trustworthiness, willingness, and ability to safeguard classified information.

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

CONCLUSIONS

I have carefully considered all the facts in evidence and the legal standards. The allegations under Guidelines M, E and K in the SOR involve the same facts. Therefore, I will address them together to reduce redundancy.

Based on all of the evidence I considered Security Violations Disqualifying Condition (SV DC)E2.A11.1.2.2 (*Violations that are deliberate or multiple or due to negligence*); Misuse of Information Technology Systems Disqualifying Condition (MI DC) E2.A13.1.2.3 (*Removal (or use) of hardware, software or media from any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations*); MI DC E2.A13.1.2.4 (*Introduction of hardware, software, or media into any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines, or regulations*), Personal Conduct (PC DC) E2.A5.1.2.1 (*Reliable, unfavorable, information provided by associates, employers, coworkers, neighbors, and other acquaintances*) and PC DC E2.A5.1.2.5 (*A pattern of dishonesty or rule violations, including violation of any written or recorded agreement made between the individual and the agency*),. and conclude they all apply. Applicant admitted to copying CDs on the company's equipment for himself and others. He admitted to viewing and editing photographs on his classified computer. Both of these actions were in violation of the rules and procedures of the company and the NISPOM. At the time he did not think he was violating any rules, although he clearly was. No evidence was presented that any of the computers were corrupted or any classified information was compromised, however there was always the potential that such could happen. His actions were deliberate, but also negligent in that he was not familiar with all of the rules regarding his use of certain equipment.

I have considered all the mitigating conditions, especially Security Violations Mitigating Condition (SV MC) E2.A11.1.3.1 (*Were inadvertent*); SV MC E2.A11.1.3.2 (*Were isolated and infrequent*); SV C E2.A11.1.3.3 (*Were due to improper or inadequate training*), SV MC E2.A11.1.3.4 (*Demonstrate a positive attitude toward the discharge of security responsibilities*); Misuse of Information Technology Systems Mitigating Conditions (MI MC) E2.A13.1.3.1 (*The misuse was not recent or significant*); MI MC E2.A13.1.3.2 (*The conduct was unintentional or inadvertent*); MI MC E2.A13.1.3.4 (*The misuse was an isolated event*); MI MC E2.A13.1.3.5 (*The misuse was followed by a prompt, good faith effort to correct the situation*), PC MC E2.A5.1.3.5 (*The individual has taken positive steps to significantly reduce or eliminate vulnerability to coercion, exploitation, or duress.*) Applicant has had a long career with his company devoid of any problems or disciplinary actions until this event. It was common practice within his office space to make copies of CDs. On many occasions his supervisor authorized the actions. Applicant was the person in the office who knew how to accomplish the task and therefore he was the one others went to for assistance to do their own copying. His actions were obviously not isolated, infrequent, or inadvertent because it went on for many years. In 2003, he was told to stop and he did. There is no evidence to support information was actually compromised. I find SV MC E2.A11.1.3.1, SV MC E2.A11.1.3.2, MI MC E2.A13.13.2 and MI C E2. A13.1.3.3 do not apply. Applicant was not hiding his actions. He did not do them in the dark of night, but accomplished them during the day when his coworkers were present. When his supervisor told him to stop, he did, except when the supervisor asked him to do something for him. Applicant should have known better, but it is clear that security training was quite lax. Once Applicant was disciplined, the company almost immediately reinforced its rules and procedures and made sure people understood what was and was not permitted. There was ample evidence to support that after Applicant was disciplined, the company increased their security training and security awareness. Applicant has been vigilant and diligent in ensuring he abides by all the rules and procedures since 2003. It is common knowledge what occurred and it is unlikely this event could be used for exploitation or makes him more vulnerable to coercion or duress. Therefore I find SV MC E2.A11.1.3.3, SV MC E2.A11.1.3.4, MI MC E2.A13.1.3.5, and PC MC E2.A5.1.3.5 apply.

I have considered all of the evidence and the disqualifying conditions under the personal conduct guideline as it pertains to Applicant taking the discarded plastic CD sleeves, and conclude none apply. The government alleged as a security concern that Applicant took for his personal use discarded plastic sleeves that belonged to the company. I find Applicant's conduct was not a violation of any rule or regulation of the company. He took out of the trash what was

thrown away. There was nothing proprietary, unique or identifiable about the sleeves. I find there is no personal conduct security concern as it relates to the CD sleeves.

In all adjudications, the protection of our national security is the paramount concern. The objective of the security-clearance process is the fair-minded, commonsense assessment of a person's life to make an affirmative determination that the person is eligible for a security clearance. Indeed, the adjudicative process is a careful weighing of a number of variables in considering the "whole person" concept. It recognizes that we should view a person by the totality of their acts, omissions, motivations and other variables. Each case must be adjudged on its own merits, taking into consideration all relevant circumstances, and applying sound judgment, mature thinking, and careful analysis.

I considered the whole person. I considered that Applicant acknowledged his mistakes, and the fact that he was not only copying for himself, but for others, including his supervisor, who gave him at least tacit and constructive approval. I also considered there was no evidence of an actual compromise of material and the security training was inadequate. I considered that Applicant had no other blemishes on his record before or after the problem arose, and he has a renewed sense of commitment to security awareness. I find Applicant mitigated the security concerns under Guidelines M, K and E. Therefore, I am persuaded by the totality of the evidence in this case, that it is clearly consistent with the national interest to grant Applicant a security clearance. Accordingly, Guideline M, K and E are decided for 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:

Paragraph 1. Guideline M: FOR APPLICANT

Subparagraph 1.a: For Applicant

Subparagraph 1.b: For Applicant

Paragraph 2. Guideline E: FOR APPLICANT

Subparagraph 2.a: For Applicant

Subparagraph 2.b. For Applicant

Paragraph 3. Guideline K: 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.

Carol G. Ricciardello

Administrative Judge

1. Exec. Or. 10865, *Safeguarding Classified Information within Industry* (Feb. 20, 1960) as amended and modified.

2. Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (Jan. 2, 1992), as amended and modified.

3. AE B.

4. AE C.

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

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

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

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

9. ISCR Case No. 93-1390 at 7-8 (App. Bd. Jan. 27, 1995); Directive, Enclosure 3, ¶ E3.1.15.

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

11. *Id*.

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

13. Executive Order 10865 § 7.