DATE: July 17, 2006

In Re:

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

Applicant for Security Clearance

CR Case No. 04-09251

DECISION OF ADMINISTRATIVE JUDGE

JOAN CATON ANTHONY

APPEARANCES

FOR GOVERNMENT

Braden M. Murphy, Esq., Department Counsel

FOR APPLICANT

Jerry R. Goldstein, Esq.

SYNOPSIS

While Applicant mitigated security concerns under Guidelines M and B of the Directive, he failed to mitigate Guideline E security concerns that he deliberately failed to disclose in an initial security interview his receipt of a letter of reprimand for misuse of a sensitive but unclassified computer network. Clearance is denied.

STATEMENT OF THE CASE

The Defense Office of Hearings and Appeals (DOHA) declined to grant or continue a security clearance for Applicant. On September 27, 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 B (Foreign Influence) of the Directive. On October 19, 2005, Applicant submitted an answer to the SOR and elected to have a hearing before an administrative judge. The case was assigned to me on February 14, 2006, and, on March 30, 2006, I convened a hearing to consider whether it is clearly consistent with the national interest to grant or continue a security clearance for Applicant. Applicant, who was represented by counsel, waived the 15-day notice provision found at ¶ E3.1.8. of Enclosure 3 of the Directive. At the hearing, the Government called no witnesses, introduced four exhibits, identified and numbered Exs. 1 through 4, and offered one document for administrative notice (Government I). The Government's exhibits and document for administrative notice were admitted to the record without objection. Applicant called no witnesses and testified on his own behalf. He introduced 13 exhibits, identified as Exs. A through M, and offered one document for administrative notice (Applicant's A-I). Applicant's exhibits and document for administrative notice were admitted to the record without objection. DOHA received the transcript (Tr.) of the proceeding on April 10, 2006.

RULINGS ON PROCEDURE

At the hearing, Department Counsel moved to amend allegation 2.b. of the SOR by adding the word initial before the words security interview. Applicant did not object to the proposed amendment, and Department Counsel's motion to amend was granted. The amended allegation 2.b. reads as follows: "During your initial security interview with an

authorized investigator of the Department of Defense, you deliberately failed to disclose the [name of agency] investigation concerning the conduct set forth in paragraph 1., above, due to your fear that this incident would negatively impact your security clearance."[(3)]

FINDINGS OF FACT

The amended SOR in this case contains one allegation of disqualifying conduct under Guideline M, Misuse of Information Technology Systems, two allegations of disqualifying conduct under Guideline E, Personal Conduct, and three allegations raising security concerns under Guideline B, Foreign Influence. In his answer to the SOR, Applicant admitted the Guideline M and E allegations. He denied allegation 3.a. and part of allegation 3.b. under Guideline B. He admitted part of allegation 3.b. and all of allegation 3.c. under Guideline B. Applicant's admissions are incorporated as findings of fact.

Applicant is 36 years old, married, and the father of three young children. He has held a security clearance since 1996. (Tr. 98-99.) For the past two years, he has been employed as a computer systems engineer by a government contractor. (Ex. 1; Tr. 69; 74-75; 88.) In June 2006, he expected to receive a bachelor of science degree with emphasis in computer networking. (Ex. B; Tr. 49; 87.)

Applicant's employment record includes twelve years of service in the U.S. military. He joined the U.S. Army in August 1991 and left active duty in September 2003. He received an honorable discharge. In April 2004, he joined the Army National Guard in his state of residence. (Ex. 1; Tr. 43; 68.)

While on active duty in the Army and assigned overseas, Applicant began to take courses that would provide him with certification as a software engineer. In 2000, Applicant returned to the U.S. and continued pursuing computer certification courses. (Ex. C; Tr. 46.) He purchased used equipment and built his own computer network at home, which enabled him to practice skills and solve problems raised in his studies. (Tr. 54.) Applicant took a course in network security which exposed the methodologies of computer system hackers. (Ex. B at 5-6.) Before taking the network security course, in an attempt to learn how to deal with hackers, Applicant downloaded hacking tools files from the Internet so he could practice hacking into his computer network at home.[(4)] He put the hacking tools files on a zip drive. (Ex. 3 at 1; Tr. 55; 129-130.)

In August 2000, the Army assigned him to teach computerized courses in graphic design and lithography. (Tr. 44; 46; 53; 100) Applicant served as an instructor until he left the Army in September 2003. During that period he taught ten different courses. One course taught by Applicant ran for sixteen weeks. In that course students learned the basics of computers and progressed to the use of computer applications in lithography. Applicant was responsible for developing his own lesson plans for his courses. (Tr. 55-57.)

Applicant and other course instructors were told to use the computer lab at work to make the lesson plans for the courses they were teaching. However, the computer labs were crowded with students, and computers were often not available to use in making lesson plans. Applicant therefore used his own disks and his home computer network to make his lesson plans. One day he made his lesson plans at home and unknowingly saved them to a disk containing the hacking tools. He took the disk to his workplace, used the files he had copied to teach his course, and left the disk on his desk. In August, 2001, while Applicant was out of the office on assignment, a co-worker borrowed the disk with the lesson plans and found the hacking tools files as well. (Ex. 3 at 1; Tr.59-61; 103-107.)

When Applicant returned to the office, his co-worker and supervisor confronted him with the fact they had found the hacking tools file on the zip drive along with his lesson plans. The supervisor notified the unit's division chief, and an investigation was begun in approximately November 2001. (Tr. 106-108.) The investigation, which concluded in approximately February 2002, found that Applicant was guilty of bringing hacking files into the agency workplace and improper personal use of his e-mail account to forward jokes, chain letters, games, and other personal messages sent to him. He did not put the hacking software on any computer application belonging to his employer. Applicant was notified of the results of the investigation in February 2002. (Ex. 3 at 1; Ex. 4; Tr. 61; 107-109.)

A higher official ordered a second investigation, which was conducted in April 2002. The conclusions of the second

investigation were essentially those of the first. In June 2002, Applicant received a local letter of reprimand,[(5)] was required to relinquish his computer account, and was not permitted to log on to any of the agency network computers. (Ex. 3 at 1; Tr. 16; 61-62.) Applicant's NCO Evaluation Report (DA Form 2166-8, Oct 2001) for the period August 2002 through July 2003 rated him as having high potential for promotion, found him to be knowledgeable and experienced in all aspects of his military occupation speciality (MOS), and recommended he be assigned to positions of greater responsibility. (Ex. D.)

Applicant completed a security clearance application in January 2002. On April 17, 2002, he was interviewed by a special investigator for the U.S. Office of Personnel Management (OPM) and provided a signed statement. In the statement, Applicant discussed his family and his wife's family situation. He did not discuss the investigation of his conduct related to bringing the zip drive containing hacking tools to his workplace or his unauthorized and personal use of his office e-mail system. He did not inform the OPM investigator that he had been notified of the results of the investigation in February 2002. (Ex. 2; Ex. 3 at 1.)

On October 31, 2002, Applicant was interviewed again by an OPM special investigator and provided a signed statement. He explained in detail the two investigations into his alleged noncompliance with rules, procedures, guidelines, or regulations pertaining to information technology systems. He specified the findings of the two investigations and the penalties assessed him. He further stated: "I did not mention this investigation during my [April 17, 2002] clearance interview, a[s] I was afraid this incident would have negatively impacted my clearance." (Ex. 3 at 2.)

Applicant and his wife were married in 1997. At the time of their marriage, Applicant's wife was a citizen of Poland and a resident of Italy. (Ex. 1; Tr. 74.) Applicant's wife became a U.S. citizen in September 2002. (Ex. I; Ex. J.) Applicant's wife's mother and two of her three brothers are citizens and residents of Poland. One of Applicant's brothers-in-law is a baker and the other is a construction worker. (Tr. 75.) Applicant's mother-in-law, a widow, works as a housekeeper and is a citizen and resident of Poland. (Tr.78-79.) She has visited Applicant and his family in the U.S. on four occasions: from November 2001 to July 2002; for about four months in 2003; for two to three weeks in 2004; and from November 2005 to February 2006. (Tr. .94-96.) When Applicant's mother-in-law resided with him and his family from November 2001 to July 2002, she helped Applicant and his wife with the care of their young children. (Tr. 78-79.) While Applicant's mother-in-law has visited him and his family three times since July 2002, he does not consider his home her residence, and she resides in Poland. (Answer to SOR, at 1.) Applicant does not expect his mother-in-law to come to the U.S. for future visits. (Tr.96.)

Applicant visited Poland in 1999. His wife speaks on the telephone once a month with her mother and her two brothers in Poland. (Tr. 79-80.) Applicant's mother-in-law receives approximately $20 a month in benefits from the government of Poland. (Tr. 93.) Applicant's wife's family members in Poland have no ties to the government of Poland. Applicant and his wife provide no support to the mother-in-law or to the brothers in Poland. (Tr. 80.)

In 2001, Applicant's wife's youngest brother, a child of approximately twelve, came to the U.S. with his mother to visit Applicant and his wife. Because the youngest brother's home life in Poland was difficult and without much adult supervision, Applicant and his wife decided to adopt him and offer him a better life in the U.S. They formally adopted the brother in July 2004. (Ex. K; Ex. L.) Applicant and his wife have applied for U.S. citizenship for their adopted son, who is now approximately 17 years old. (Ex. M; Tr. 76-77; 90.)

Applicant submitted performance evaluations from his military service and his work as a government contractor. His supervisors evaluated his performance of his duties and his work ethic at consistently high levels. (Ex. D; Ex. E; Ex. F.) Former co-workers and supervisors submitted letters of character reference on behalf of Applicant that uniformly praised his dedication, skill as a teacher, and ability to motivate others. (Ex. G) One of his former military commanders described him as "the epitome of professionalism" and a "NCO of truly extraordinary character." (Ex. G at 3.)

I take administrative notice that Poland is a stable country with a free-market economy. (U.S. Department of State, Consular Information Sheet: Poland, January 30, 2006: Government document for administrative notice I.) Poland is a member of the European Union, the North Atlantic Treaty Organization, and is allied with the U.S. in the Iraq war. (The World Factbook: Poland: http://www.cia.gov/cia/publications/factbook/geos/pl.html : Applicant's document for

administrative notice A I at 2; Tr. 86.)

POLICIES

"[N]o one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988). As Commander in Chief, 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." *Id.* at 527. The President has restricted eligibility for access to classified information to United States citizens "whose personal and professional history affirmatively indicates loyalty to the United States, strength of character, trustworthiness, honesty, reliability, discretion, and sound judgment, as well as freedom from conflicting allegiances and potential for coercion, and willingness and ability to abide by regulations governing the use, handling, and protection of classified information." Exec. Or. 12968, *Access to Classified Information* § 3.1(b) (Aug. 4, 1995). Eligibility for a security clearance is predicated upon the applicant meeting the security guidelines contained in the Directive.

Enclosure 2 of the Directive sets forth personal security guidelines, as well as the disqualifying conditions and mitigating conditions under each guideline. In evaluating the security worthiness of an applicant, the administrative judge must also assess the adjudicative process factors listed in ¶ 6.3 of the Directive. The decision to deny an individual a security clearance is not necessarily a determination as to the loyalty of the applicant. *See* Exec. Or. 10865 § 7. 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 establish, by substantial evidence, conditions in the personal or professional history of the applicant that disqualify, or may disqualify, the applicant from being eligible for access to classified information. *See Egan*, 484 U.S. at 531. The Directive presumes a nexus or rational connection between proven conduct under any of the disqualifying conditions listed in the guidelines and an applicant's security suitability. *See* ISCR Case No. 95-0611 at 2 (App. Bd. May 2, 1996).

Once the Government establishes a disqualifying condition by substantial evidence, the burden shifts to the applicant to rebut, explain, extenuate, or mitigate the facts. ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002); *see* Directive ¶ E3.1.15. An applicant "has the ultimate burden of demonstrating that it is clearly consistent with the national interest to grant or continue his security clearance." ISCR Case No. 01-20700 at 3.

CONCLUSIONS

Guideline M - Misuse of Information Technology Systems

In the SOR, DOHA alleged under Guideline M of the Directive that in June 2002, Applicant received a Letter of Reprimand for misuse of a sensitive but unclassified computer network, for bringing hacking software into the workplace, and for misuse of his e-mail account, conduct that caused his access to the sensitive but unclassified computer network to be suspended indefinitely. (¶ 1.a.).

Pursuant to the Directive, information technology systems are defined as "all related equipment used for the communication, transmission, processing, manipulation, and storage of classified or sensitive information." E2. A13.1.1. The Government's concern under Guideline M is that a person's noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about his trustworthiness, willingness, and ability to properly protect classified systems, networks, and information.

Applicant's conduct raises security concerns under Disqualifying Conditions (DC) E2.A.13.1.2.2. and E2.A13.1.2.4. of Guideline M. Applicant prepared his lesson plans at home on his personal computer network and copied them onto a file that also contained hacking software he had downloaded from the internet. Applicant brought the file with the lesson plans and the hacking software to his workplace. While there was no evidence he used the hacking software at his workplace, the hacking software was on the file he used for making his lesson plans, and the lesson plans were placed on the employer's sensitive computer network, raising a concerns under DC E2.A13.1.2.4. When Applicant forwarded inappropriate non-work-related e-mails from his account on his employer's sensitive but unclassified computer network,

he was making unauthorized modifications or manipulations of information residing on the employer's information technology system, thus raising a concern under DC E2.A13.1.2.2.

I have reviewed the relevance of Applicant's conduct in light of Guideline M disqualifying and mitigating conditions. I have also weighed his conduct and reliable information about him, past and present, favorable and unfavorable, in light of the nine factors, identified at E2.2.1. of the Directive, as comprising the whole person concept. I conclude Applicant's misuse of his employer's computer system was not recent, nor was it significant. He supplied credible testimony to show his conduct was unintentional and inadvertent. His misuse of his employer's information technology system was limited to these isolated events. Accordingly, Mitigating Conditions (MC) E2.A.13.1.3.1., E2.A.13.1.3.2., and E2.A.13.1.3.4. apply to the facts of Applicant's case. I conclude that Applicant has mitigated the disqualifying conduct alleged in ¶ 1.a. of the SOR

Guideline E - Personal Conduct

Guideline E conduct raises security concerns because it involves questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations and could indicate that an applicant may not properly safeguard classified information. Directive ¶ E2.A5.l.l.

Applicant's conduct raises security concerns under Guideline E Disqualifying Conditions (DC) E2.A5.1.2.1., E2.A5.1.2.3., E2.A5.1.2.4., and E2.A5.1.2.5. In ¶1.a. of the SOR DOHA alleged Applicant copied his lessons plans to a file containing hacking tools and brought the file to his workplace, where it was discovered by a co-worker and a supervisor. An investigation by the employer also revealed Applicant forwarded personal communications such as games, jokes, and chain letters from the e-mail account provided to him by his employer for carrying out official business. This conduct violated workplace rules and raises security concerns under DC E2.A5.1.2.5. of Guideline E.

Additionally, Applicant's responses in his initial security interview on April 17, 2002 with an authorized investigator raise security concerns under E2.A5.1.2.3. and E2.A5.1.2.4. In February 2002, Applicant was notified of the results of his employer's investigation of the disqualifying conduct alleged under Guideline M of the Directive. In his signed, sworn statement of October 31, 2002, Applicant admitted he deliberately failed to disclose the information in his April 17, 2002 interview because he feared it would have a negative impact on his security clearance.

We turn to an examination of possible Mitigating Conditions (MC) under the Guideline. The information about Applicant's unprofessional conduct that was provided by Applicant's coworkers and employers was pertinent to a determination of his judgment, trustworthiness, or reliability. Therefore, MC E2.A5.1.3.1 is inapplicable. Additionally, MC E2.A5.1.3.2. applies only in part to Applicant's case because his falsification, while not recent and an isolated incident, was not corrected voluntarily. Since Applicant did not make a prompt good-faith effort to correct the falsification before being confronted with the facts, MC E2.A5.1.3.3. is also inapplicable. Applicant's performance evaluation for the period 2002 and 2003 and his conduct in carrying out his work after the investigation indicate he had taken positive steps to demonstrate his reliability and trustworthiness and to reduce or eliminate his vulnerability to coercion, exploitation, or duress. Thus, MC E2.A5.1.3.5. is applicable.

Even though Applicant provided some mitigation for the Guideline E disqualifying conditions, the mitigation is not sufficient to overcome the Government's concerns raised by his deliberate misrepresentations in his initial security interview. Applicant's lack of candor with the Government suggests he may put his own concerns before his obligation to safeguard classified information. The ability to be truthful goes to the essence of an individual's security worthiness. With respect to the Guideline E conduct alleged in the SOR, the Government has established its case. Accordingly, the allegations in subparagraphs 2.a. and 2.b. of the SOR are concluded against the Applicant.

Guideline B - Foreign Influence

In the SOR, DOHA alleged, under Guideline B of the Directive, that Applicant's wife was a citizen of Poland and resided with him in the United States (¶ 3.a.); that Applicant's mother-in-law and brother-in-law were citizens of Poland and resided with him in the United States (¶ 3.b.); and that Applicant had two brothers-in-law who are citizens and residents of Poland (¶3.c.). At his hearing, Applicant submitted evidence showing his wife became a U.S. citizen on September 26, 2002 and was issued a U.S. passport on November 5, 2002. (Ex. I; Ex. J.) He testified that his mother-in-

law, who had visited his family in the U.S. four times since 2001, had returned to Poland and was residing there. He also submitted evidence showing he and his wife had adopted the wife's youngest brother, that an adoption order was issued by their county circuit court on July 26, 2004, and that Applicant and his wife were pursuing U.S. citizenship for their adopted son. (Ex. K; Ex. L; Ex. M.) Applicant supplied credible evidence to rebut allegation 3.a. and part of allegation 3.b of the SOR. Thus, only part of SOR allegation 3.b. and SOR allegation 3.c. remain to be considered in this case.

A Guideline B security concern exists when an individual seeking clearance is bound by ties of affection, influence, or obligation to immediate family, close friends, or professional associates in a foreign country, or to persons in the United States whose first loyalties are to a foreign country. A person who places a high value on family obligations or fidelity to relationships in another country may be vulnerable to duress by the intelligence service of the foreign country or by agents from that country engaged in industrial espionage, terrorism, or other criminal activity. The more faithful an individual is to family ties and obligations, the more likely the chance that the ties might be exploited to the detriment of the United States.

Applicant's case requires the recognition that the government of Poland is a democratic fee-market country with a stable government. Poland is a member of the North Atlantic Treaty Organization (NATO), a member nation in the European Union, and is allied with the U.S. in the Iraq war.

Applicant's admissions raise two possible Guideline B security concerns. Applicant has a mother-in-law and two brothers-in-law who are citizens and residents of Poland, suggesting a security concern under E2.A2.1.2.1. of Guideline B. Additionally, Applicant's wife, with whom he shares his home, has close ties of affection and obligation to her mother and brothers who are citizens and residents of Poland, a situation with the potential for foreign influence or duress, and this raises a security concern under E2.A2.1.2.2. of Guideline B.

An applicant may mitigate foreign influence security concerns by demonstrating that immediate family members are not agents of a foreign power or in a position to be exploited by a foreign power in a way that could force an applicant to choose between loyalty to the foreign associates and loyalty to the U.S. Mitigating Condition (MC) E2.A2.1.3.1. Applicant's mother-in-law is employed as a domestic worker in Poland. His brothers-in-law are also employed in Poland; one works as a cook; the other as a construction worker. Poland is a stable democratic society and an ally of the U.S. The evidence does not establish that Applicant's mother-in-law and brothers-in-law are agents of a foreign power and nothing in the record supports a conclusion that the mother-in-law and brothers-in-law are in positions to be exploited by a foreign power in a way that could force Applicant to choose between loyalty to his wife, mother-in-law, and brothers-in-law and the United States.

However, foreign connections derived from marriage and not from birth can raise Guideline B security concerns. In reviewing the scope of MC E2.A2.1.3.1., DOHA's Appeal Board has stated that the term "associate(s)" reasonably contemplates in-laws and close friends. ISCR Case No. 02-12760 at 4 (App. Bd. Feb. 18, 2005) Accordingly, MC E2.A2.1.3.1. does not apply to Applicant's case.

An applicant may also mitigate foreign influence security concerns if he shows his contacts and correspondence with foreign citizens are casual and infrequent. MC E2.A2.1.3.3. Applicant is committed to his wife, a relationship that is enduring and familial. His wife's contacts with her mother and two siblings who are citizens and residents of Poland are based on family obligations and affection and are therefore not casual. Applicant's wife speaks with her mother and brothers in Poland once a month by telephone. She is aware of their needs and her obligations to them. Accordingly, C E2.A2.1.3.3. does not apply to Applicant's relationship with his mother-in-law and brothers-in-law in Poland.

In assessing Applicant's potential for adverse foreign influence, I have balanced all the factual circumstances and applied them to the adjudicative criteria established in the Directive in light of the whole person concept. I considered the likelihood that the government of Poland or a foreign power operating in Poland would exploit Applicant's mother-in-law and brothers-in-law, their vulnerability to pressure, coercion, or duress, and Applicant's ties of affection or obligation to his wife's relatives and to the United States. I conclude that Applicant provided credible evidence to mitigate the security concerns discussed herein and demonstrate that he would not be vulnerable to foreign influence that would result in the compromise of classified information. Accordingly, the allegations in subparagraphs 3.a., 3.b., and 3.c. of the SOR are concluded for the Applicant.

In all adjudications, the protection of our national security is the paramount concern. Security clearance decisions are not intended to assign guilt or to impose further punishment for past transgressions. Rather, the objective of the security clearance process is the fair-minded, common sense assessment of a person's trustworthiness and fitness for access to classified information. Indeed, the "whole person" concept recognizes we should view a person by the totality of his or her acts and omissions, including all disqualifying and mitigating conduct. Having done so, I conclude Applicant should not be entrusted with a security clearance. In reaching my decision, I have considered the evidence as a whole, including the appropriate factors and guidelines in Department of Defense Directive, 5220.6., as amended.

FORMAL FINDINGS

The following are my conclusions as to the allegations in the SOR:

Paragraph 1: Guideline M: FOR APPLICANT

Subparagraph 1.a.: For Applicant

Paragraph 2.: Guideline E: AGAINST APPLICANT

Subparagraph 2.a.: Against Applicant

Subparagraph 2.b. Against Applicant

Paragraph 3.: Guideline B: FOR APPLICANT

Subparagraph 3.a.: For Applicant

Subparagraph 3.b.: For Applicant

Subparagraph 3.c.: For Applicant

DECISION

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

Joan Caton Anthony

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. The evidence showed the authorized investigators who interviewed Applicant on April 17, 2002, and October 31, 2002, were Special Investigators for the Office of Personnel Management Investigations Service.

4. Applicant produced a syllabus for a course he took on computer network safety from April 1 to June 10, 2003. The course contained segments relating to hacking. (Ex. B.)

5. Applicant testified that a local letter of reprimand was a disciplinary action for a work rule violation. The local letter of reprimand did not go into an individual's permanent military record or personnel file , but stayed within the command for two years, whereupon it was destroyed. Tr. 62-65.