DATE: December 27, 2006

In re:

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

Applicant for Security Clearance

CR Case No. 05-01154

DECISION OF ADMINISTRATIVE JUDGE

MARK W. HARVEY

APPEARANCES

FOR GOVERNMENT

Eric H. Borgstrom, Esq., Department Counsel

FOR APPLICANT

Lawrence D. Kerr, Esq.

SYNOPSIS

Sixty-one-year-old Applicant was a Facility Security Officer (FSO) for six years. She was primarily responsible for enforcing security requirements in her workplace. She asked the Defense Security Service (DSS) Industrial Security Representative (ISR) about obtaining accreditation for her employer's laptop computer. The DSS ISR told her the references for accomplishing this objective, but she was unable to understand and complete requirements. She authorized contractor's employees to place classified information on the unaccredited, laptop computer on ten occasions, and then self-reported the security violations. She failed to mitigate security concerns pertaining to security violations. Clearance is denied.

STATEMENT OF THE CASE

On January 10, 2003, Applicant applied for a security clearance and submitted a Security Clearance Application (SF 86).[(1)] On October 11, 2005, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) to her, pursuant to Executive Order 10865, *Safeguarding Classified Information Within Industry,* dated February 20, 1960, as amended and modified, and Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (Directive), dated January 2, 1992, as amended and modified.[(2)] The SOR alleges security concerns under Guidelines K (Security Violations), and E (Personal Conduct). 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 her, and recommended referral to an administrative judge to determine whether a clearance should be granted, continued, denied, or revoked.

In a sworn answer on November 16, 2005, Applicant responded to the SOR allegations, and elected to have her case decided at a hearing.[(3)] On September 21, 2006, the case was assigned to me and on November 8, 2006, the hearing was held. On November 28, 2006, DOHA received the transcript, and on December 8, 2006, it was provided to me.

PROCEDURAL RULING

At the hearing, Department Counsel asked for administrative notice of Exhibit I (R. 13-14). Exhibit I is the National Industrial Security Program Operating Manual, DoD 5220.22-M, dated January 1995, with Change 1 (July 1997) and Charge 2 (Feb. 2001) (NISPOM), a total of 44 pages. Administrative or official notice is the appropriate type of notice used for administrative proceedings. *See* ISCR Case No. 02-24875 at 2 (App. Bd. Oct. 12, 2006) (citing ISCR Case No. 02-18668 at 3 (App. Bd. Feb. 10, 2004); *McLeod v. Immigration and Naturalization Service*, 802 F.2d 89, 93 n.4 (3d Cir. 1986)). The most common basis for administrative notice at ISCR proceedings, is to notice facts that are either well known, or from government publications or government reports. *See* Stein, Administrative Law, Section 25.01 (Bender & Co. 2006) (listing fifteen types of facts for administrative notice). Applicant did not object to my consideration of Exhibit I, and I approved administrative notice of Exhibit I (R. 13-14).

FINDINGS OF FACT

Applicant admitted that she violated security rules as alleged in the SOR ¶1.a, but denied that security was compromised and that her personal conduct has detrimental security implications as alleged in SOR ¶ 2.a. She explained that she self-reported the security violation, and disclosed other extenuating circumstances and mitigating information. Her admissions are incorporated herein as findings of fact.[(4)]

Applicant is 61-years-old.[(5)] She received a secret clearance from the Federal Bureau of Investigation in 1963, a confidential clearance from Department of Energy in 1978, and a secret clearance from the Department of Defense (DoD) in 1983. Her clearance as well as the clearance for the contractor's facility was downgraded to confidential in 1992 because there was no need to use secret information (R. 38, 53). She has been employed as a contract administrator and facility security officer (FSO) for the same defense contractor for the last six years.[(6)] She has attended college courses, but did not receive a college degree.[(7)] She has no prior military service.[(8)]

As FSO, she was responsible for directing "security measures as necessary for . . . safeguarding information."[(9)] She is "responsible for safeguarding classified information entrusted to [her]. The extent of protection afforded classified information shall be sufficient to reasonably foreclose the possibility of its loss or compromise." NISPOM, paragraph 5-100. The data protection, data integrity, and auditing requirements for multi-user systems,[(10)] such as a laptop computer used by multiple employees are extensive. *See* NISPOM, Chapter 8, Section 6. The primary purpose of accrediting a computer is to set up software that will assist in identifying users, and the manner of the computer's use for auditing purposes (R. 23-24).

In April 2003, Applicant, acting in her role as FSO asked a Defense Security Service (DSS) Industrial Security Representative (ISR) about the procedure for establishing or accrediting a computer for classified information (R. 19, 24). The DSS ISR told her that Chapter 8 of the NISPOM and a website would have the information she needed for accreditation of her employer's computer, but he would not help her prepare the computer for accreditation (R. 19, 57-60). She was concerned about her company's requirement to get reports completed on time (R. 54). She sought the assistance of several technical assistants, but was unable to meet the technical requirements to get the computer accredited (R. 31). She asked the Navy for help, but they declined to provide any assistance developing the accreditation (R. 47). She did not understand and was not adequately trained concerning the information technology and security requirements (R. 25, 39, 40, 43; Exhibit 5, at 11).

Applicant put a label on a laptop computer stating it contained confidential, restricted data (R. 40), but it did not have the DoD warning banner on the monitor's screen (R. 52). With respect to the laptop computer, the accreditation process would have resulted in a better password, and a more secure operating system and security system (R. 49-50). The laptop computer was never connected to a network (R. 42). From late May 2003 until mid-July 2003, she authorized two other employees to use the unaccredited, laptop computer in lieu of a typewriter to prepare three reports each totaling about 100-pages which each contained a total of about two pages of classified sections (R. 39, 41, 56; Exhibit 5, at 5, 7-8, 10-11). She logged the computer out to two employees a total of ten occasions (R. 72-74; Exhibit 5, at 13). The two employees who used the unaccredited, laptop computer were cleared to the confidential clearance level (Exhibit 5, at 5, 8). The material on the computer was classified at the confidential level. She limited access to the unaccredited, laptop computer using a password, and stored it in a locked office within a closed area secured with a

combination lock (R. 40-41).

On July 28, 2003, she self-reported that she had used an unaccredited computer to process classified information because her conscience was bothering her and she believed she would get caught (R. 20, 25, 27, 60-61; Exhibit 5, at 2-3). The DSS ISR initiated an Administrative Inquiry concerning the alleged security violation (R. 20-21), which was followed by an additional, more formal investigation (R. 21). During the investigation, she admitted that she allowed two cleared employees to load classified information on the unaccredited computer on about ten occasions (R. 22, 24, 26). The investigations established that no classified material was compromised (R. 25, 26). The DSS ISR concluded Applicant was truthful in the investigation (R. 27).

After July 28, 2003, she continued to seek accreditation of the laptop computer, but her lack of understanding of the technical requirements for accreditation delayed the accreditation. Assembling the documentation and establishing the security requirements to obtain classified accreditation for a multi-user computer is onerous, especially for personnel who lack information technology training and experience (R. 67-70). Before, during and after the investigation, when not being used the computer concerned was kept locked in a security container at the company (R. 25). In February 2006, after receiving additional training and some assistance, the computer received interim accreditation (R. 22, 44-45, 57). There were no other security violations aside from those in 2003 (R. 28). Her clearance was not suspended after the investigation (R. 30, 45-46).

Applicant is an outstanding worker (R. 76). She is reliable, trustworthy and honest (R. 76-77). The investigation of security violations made her more conscientious about enforcing security requirements, and caused greater security awareness in her company (R. 46, 77). She is now a better FSO because she is more scrupulous and meticulous about her FSO duties. *Id*.

POLICIES

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

These adjudicative guidelines are not inflexible ironclad rules of law. Instead, recognizing the complexities of human behavior, an administrative judge should apply these guidelines in conjunction with the factors listed in the adjudicative process provision in Section E2.2, Enclosure 2, of the Directive. An administrative judge's overarching adjudicative goal is a fair, impartial and common sense decision.

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

Specifically, an administrative judge should consider the nine adjudicative process factors listed at Directive ¶ E2.2.1: (1) the nature, extent, and seriousness of the conduct; (2) the circumstances surrounding the conduct, to include knowledgeable participation; (3) the frequency and recency of the conduct; (4) the individual's age and maturity at the time of the conduct; (5) the voluntariness of participation; (6) the presence or absence of rehabilitation and other pertinent behavioral changes; (7) the motivation for the conduct; (8) the potential for pressure, coercion, exploitation, or duress; and (9) the likelihood of continuation or recurrence.

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

Since the protection of the national security is the paramount consideration, the final decision in each case is arrived at by applying the standard that the issuance of the clearance is "clearly consistent with the interests of national security." In reaching this decision, I have drawn only those conclusions that are reasonable, logical and based on the evidence contained in the record. Likewise, I have avoided drawing inferences grounded on mere speculation or conjecture.

In the decision-making process, facts must be established by "substantial evidence.[(11)] The government initially has the burden of producing evidence to establish a case which demonstrates, in accordance with the Directive, that it is not clearly consistent with the national interest to grant or continue an applicant's access to classified information. Once the government has produced substantial evidence of a disqualifying condition, the burden shifts to Applicant to produce evidence and prove a mitigating condition. Directive ¶ E3.1.15 provides, "The applicant is responsible for presenting witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by applicant or proven by Department Counsel, and [applicant] has the ultimate burden of persuasion as to obtaining a favorable clearance decision." The burden of disproving a mitigating condition never shifts to the government. *See* ISCR Case No. 02-31154 at 5 (App. Bd. Sep. 22, 2005).[(12)]

A person who seeks access to classified information enters into a fiduciary relationship with the government predicated upon trust and confidence. It is a relationship that transcends normal duty hours and endures throughout off-duty hours as well. It is because of this special relationship the government must be able to repose a high degree of trust and confidence in those individuals to whom it grants access to classified information. Decisions under this Directive include, by necessity, consideration of the possible risk an applicant may deliberately or inadvertently fail to protect or safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation as to potential, rather than actual, risk of compromise of classified information.

The scope of an administrative judge's decision is limited. Applicant's allegiance, loyalty, and patriotism are not at issue in these proceedings. Section 7 of Executive Order 10865 specifically provides industrial security clearance decisions shall be "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." Security clearance decisions cover many characteristics of an applicant other than allegiance, loyalty, and patriotism. Nothing in this Decision should be construed to suggest that I have based this decision, in whole or in part, on any express or implied determination as to Applicant's allegiance, loyalty, or patriotism.

CONCLUSIONS

Upon consideration of all the facts in evidence, and after application of all appropriate legal precepts, factors, and conditions, including those described briefly above, I conclude the following with respect to the allegations set forth in the SOR:

Security Violations

Under Guideline K, the Department of Defense is concerned that noncompliance "with security regulations raises doubt about an individual's trustworthiness, willingness, and ability to safeguard classified information." Directive ¶ E2.A11.1.1.

There are two security violations disqualifying conditions (SV DC) listed in Directive ¶ E2.A11.1.2, but only one potentially raises a security concern and may be disqualifying in this case. SV DC 2 applies where there have been violations "that are deliberate or multiple or due to negligence." Directive ¶ E2.A11.2.2. Applicant deliberately and knowingly violated the NISPOM on multiple (ten) occasions by authorizing employees to place classified information on an unaccredited, laptop computer.

Any of four security violations mitigating conditions (SV MC) could potentially mitigate security concerns. For SV MCs 1-3 to be applicable the security violation must be "inadvertent" (Directive ¶ E2.A11.3.1), "isolated or infrequent" (Directive ¶ E2.A11.3.2), or "due to improper or inadequate training" (Directive ¶ E2.A11.3.3). For SV MC 4 to apply, Applicant must "demonstrate a positive attitude towards the discharge of security responsibilities." Directive ¶ E2.A11.3.4. SV MCs 1-3 do not apply because the ten security violations were a deliberate and knowing decision to violate the NISPOM after the DSS ISR specifically told her about the accreditation requirements. Their temporal proximity to each other as compared to her long history of compliance with security requirements are not sufficient to merit application of SV MC 2, but do merit credit in the whole person analysis.

SV MC 4 applies to this case. After July 28, 2003, she renewed her commitment to security. She was remorseful about her security violations and redoubled her emphasis on being more conscientious about security. She is a devoted

employee who is trustworthy and serious about security. She has a positive attitude and has taken demonstrative and positive steps in discharging her security responsibilities. However, in ISCR Case No. 04-04264 at 3-4 (App. Bd. Sep. 8, 2006) the Appeal Board stated:

Security violations are one of the strongest possible reasons for denying or revoking access to classified information, as they raise very serious questions about an applicant's suitability for access to classified information. ISCR Case No. 97-0435 at 3-4 (App. Bd. July 14, 1998). Once it is established that [a]pplicant has committed a security violation, he has "a very heavy burden of demonstrating that [he] should be entrusted with classified information. Because security violations strike at the very heart of the industrial security program, an Administrative Judge must give any claims of reform and rehabilitation strict scrutiny." ISCR Case No. 00-0030 at 7 (App. Bd. Sept. 20,2001). In many security clearance cases, applicants are denied a clearance for having an indicator of a risk that they might commit a security violation (e.g., alcohol abuse, delinquent debts or drug use). Here the issue is not merely an indicator, rather the Judge found [a]pplicant disregarded in-place security procedures in violation of the NISPOM.

While I conclude that VC MC 4 is applicable in mitigation, I also conclude that, it is of insufficient weight to overcome the disqualifying conduct. Accordingly, SOR allegation 1.a. under Guideline K of the Directive is concluded against Applicant.

Personal Conduct

Under Guideline E, "conduct involving questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations could indicate that applicant may not properly safeguard classified information." Directive ¶ E2.A5.l.l.

One personal conduct disqualifying condition (PC DC) could potentially raise a security concern and may be disqualifying in this case.[(13)] PC DC 5 applies where an applicant has "a pattern of dishonesty or rule violations." Directive ¶ E2.A5.1.2.5. For SOR ¶ 2.a, Applicant's ten violations of the NISPOM are a pattern of rule violations. *See* ISCR Case No. 00-0030 at 6 (App. Bd. Sep. 20, 2001) (describing as rational the Judge's conclusion that several security violations in connection with a five-day meeting were a "pattern of rule violations").

A security concern based on Guideline E may be mitigated by substantial evidence of any of seven personal conduct mitigating conditions (PC MC). Under PC MC 1, security concerns may be mitigated when the derogatory "information was unsubstantiated or not pertinent to a determination of judgment, trustworthiness, or reliability." Directive ¶ E2.A5.1.3.1. The security violations as alleged in SOR ¶ 2.a are established by substantial evidence, and they pertain to information that was substantiated and pertinent to a determination of judgment, trustworthiness, or reliability. Accordingly PC MC 1 does not apply.

Security concerns can be mitigated under PC MC 5 when an applicant "has taken positive steps to significantly reduce or eliminate vulnerability to coercion, exploitation, or duress." Directive ¶ E2.A5.1.3.5. On July 28, 2003, Applicant disclosed the security violations, and she is not currently vulnerable to coercion, exploitation or duress. This mitigating condition primarily relates to PC DC 1, rather than PC DC 5. Nevertheless, her disclosure and candid, cooperation is sufficient to support partial application of PC MC 5. She also deserves some credit under the "whole person" concept for providing accurate information throughout the investigation and at her hearing.

While Applicant's six-week series of security violations reflect questionable judgment, untrustworthiness, unreliability, and unwillingness to comply with rules and regulations, they are relatively isolated offenses and somewhat remote in time. Directive ¶¶ 6.3.1 and 6.3.2. Moreover, her timely and accurate disclosure of the security violations has eliminated her vulnerability to coercion, exploitation, or duress and mitigated security concerns under Guideline E.

"Whole Person" Analysis

In addition to the enumerated disqualifying and mitigating conditions as discussed previously, I have considered the general adjudicative guidelines related to the whole person concept under Directive provision E2.2.1. As noted above, Applicant's security violations were serious and premeditated. Throughout the six-week period in 2003 when she was authorizing security violations, she had every opportunity to reconsider her choices. E2.2.1.1. Her actions concerning

the security violations were knowledgeable and voluntary. She knew she was not supposed to permit classified information on the unaccredited, laptop computer, but she authorized it anyway. E2.2.1.2 and E2.2.1.5. She committed ten violations in a six-week period ending on July 28, 2003. Applicant has held a clearance for more than 40 years. Thus, her relatively brief period of security violations must be balanced against her overall security history. E2.2.1.3. She was in his late 50's when she made the security violations and was sufficiently mature to be fully responsible for her conduct. E2.2.1.4. She authorized the security violations so that her company could meet a deadline for several reports, and as such she was not motivated by any desire to harm her country or national security. E2.2.1.7. After July 28, 2003, her behavior changed-she learned from her mistakes and has an enhanced, conscientious desire to protect and safeguard national security. Her decision-making process is sensitized to security concerns. The likelihood or potential of future security violations is low because of her positive attitude towards security. She provided sufficient evidence of her commitment to ensuring security is protected. There is no potential for pressure, coercion, exploitation or duress. E2.2.1.6, E2.2.1.8 and E2.2.1.9.

Applicant also argued for consideration of the adjudicator considerations in Directive provision E2.2.5, and the Appeal Board has noted their relevancy to the decision process in ISCR Case No. 04-00631 at 4 (App. Bd. Sep. 6, 2006) and ISCR Case No. 98-0394 at 4 (App. Bd. June 10, 1999). She voluntarily, truthfully, and completely reported the security violations on July 28, 2003, and thereafter during the subsequent investigations. She was fully truthful and candid at the hearing. She followed the guidance of the DSS ISO after July 28, 2003. Even while the security violations were occurring, she undertook some measures to ensured no classified information was compromised. Her conduct favorably resolved the security concern because she ensured the laptop was secured until it was accredited in 2006. She demonstrated positive changes in behavior and employment. Moreover, the government did not suspend her clearance in 2003 when the violations were recent and her track record of change and rehabilitation were not yet established.

Her evidence that she has learned from her mistakes and has an enhanced, conscientious desire to protect and safeguard national security is her strongest evidence of mitigation, but her multiple breaches of her FSO responsibility to enforce security requirements weighs heavily against her. After weighing the disqualifying and mitigating conditions, all the facts and circumstances, in the context of the whole person, I conclude Applicant has not mitigated the security concerns pertaining to security violations, but she has mitigated security concerns regarding personal conduct.

The evidence leaves me with grave questions and doubts as to Applicant's security eligibility and suitability. I take this position based on the law, as set forth in *Department of Navy v. Egan,* 484 U.S. 518 (1988), my "careful consideration of the whole person factors"[(14)] and supporting evidence, my application of the pertinent factors under the Adjudicative Process, and my interpretation of my responsibilities under Enclosure 2 of the Directive. Applicant has failed to mitigate or overcome the government's case. 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 K: AGAINST APPLICANT

Subparagraph 1.a: Against Applicant

Paragraph 2, Guideline E: FOR APPLICANT

Subparagraph 2.a: For Applicant

DECISION

In light of all 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.

Mark W. Harvey

Administrative Judge

1. Exhibit 1, Electronic Standard Form (SF) 86, Security Clearance Application is dated January 10, 2003. There is no allegation of falsification of this SF 86 in the statement of reasons (SOR).

2. Exhibit 7 (Statement of Reasons (SOR), dated October 11, 2005) at 1-2. Exhibit 7 is the source for the remainder of this paragraph.

3. Exhibit 8, Applicant's response to SOR, dated November 16, 2005.

4. Exhibit 8, *supra* note 3, is the source for all factual assertions in this paragraph.

5. Exhibit 1, *supra* note 1, section 1.1, at 1; R. 53.

6. *Id.*, section 6.1, at 1; R. 37.

7. *Id*., section 5.1, at 1.

8. *Id*., section 11, at 3.

9. R. 32; Exhibit 2 (Contractor's Standard Practice Procedure for Safeguarding Classified Information (Oct. 1993)), at paragraph 1.2.

10. NISPOM, para. 8-501 provides, "[s]ystems that have one user at a time, but have a total of more than one user with no sanitization between users, are multi-user systems."

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

12. "The Administrative Judge [] consider[s] the record evidence as a whole, both favorable and unfavorable, evaluate[s] Applicant's past and current circumstances in light of pertinent provisions of the Directive, and decide[s] whether Applicant ha[s] met his burden of persuasion under Directive ¶ E3.1.15." ISCR Case No. 04-10340 at 2 (App. Bd. July 6, 2006).

13. PC DC 1 does not apply because Applicant disclosed the unfavorable information about her security violations. *See* Directive ¶ E2.A5.1.2.1.

14. *See* ISCR Case No. 04-06242 at 2 (App. Bd. June 28, 2006).