DATE: December 27, 2004

In Re:

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

Applicant for Security Clearance

ISCR Case No. 03-19075

ECISION OF ADMINISTRATIVE JUDGE

LEROY F. FOREMAN

APPEARANCES

FOR GOVERNMENT

Edward W. Loughran, Esq, Department Counsel

FOR APPLICANT

Sheldon I. Cohen, Esq.

SYNOPSIS

Applicant was involved in three incidents involving classified materials: (1) she forgot to secure her safe on one occasion; (2) she inadvertently moved classified material to an unclassified computer because a colleague failed to identify the material as classified; and (3) she failed to double-check a colleague's safe at the end of the day, as required by local security procedures. Security concerns under Guidelines K and E are mitigated. Clearance is granted.

STATEMENT OF THE CASE

On June 24, 2004, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) detailing the basis for its decision to revoke Applicant's security clearance. This action was taken under Executive Order 10865, *Safeguarding Classified Information within Industry* (Feb. 20, 1960), as amended and modified, and Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (Jan. 2, 1992), as amended and modified (Directive). The SOR alleges security concerns under Guidelines K (Security Violations) and E (Personal Conduct) of the Directive. Applicant answered the SOR in writing on July 21, 2004. She admitted the specific allegations in the SOR, denied that her conduct raised security concerns, offered explanations, and requested a hearing. The case was assigned to me on August 31, 2004. On September 1, 2004, DOHA issued a notice of hearing setting the case for October 7, 2004. I conducted the hearing as scheduled. DOHA received the transcript (Tr.) on October 26, 2004.

FINDINGS OF FACT

Applicant's admissions in her answer to the SOR and at the hearing are incorporated into my findings of fact. I also make the following findings:

Applicant is a 42-year-old computer software engineer. She is employed as a principal engineer manager for a defense contractor. She has worked for her present employer for ten years. She has worked as a computer software engineer for more than 20 years. She has a bachelor of science degree in electrical and computer engineering, a master's degree in

electrical engineering, and a master's degree in systems engineering. She has held a security clearance for five years.

Applicant is a single parent and adoptive mother of a 14-year-old boy. She also has a 3-year-old boy and a one-year-old girl. She is very active in community affairs and holds positions of trust in civic organizations.

Applicant's work site consists of a classified laboratory and an unclassified laboratory. About ten to fifteen employees work in the classified laboratory. There are four safes and 20-25 computers in the classified area, which is protected by a dial lock, number lock, and an electronic alarm system.

On June 27, 2002, Applicant opened a safe in a classified laboratory and forgot to lock it when she left the laboratory for lunch. She locked the laboratory when she left. A security specialist conducting a spot check noticed the unlocked safe. The security specialist secured the safe and determined that no classified information was compromised. Although Applicant had a security clearance for about three years before this incident, this was her first classified project, and she was not yet accustomed to the security routine. Her supervisor discussed the incident with her, and he described her reaction as "very embarrassed." She accepted responsibility and promised that it would not happen again. No formal action was taken against her. This incident is the basis for the SOR ¶ 1.c.

On August 16, 2002, Applicant was asked by a colleague to move four files, believed to be unclassified, from a classified computer to an unclassified computer. At the time, the laboratory was working on a cell phone that could be used for unclassified conversations and encrypted for classified conversations. The operational "keys" for enabling and disabling encryption were classified. Unclassified keys were also produced to allow integration of internal components and testing of the equipment in an unclassified environment. Because the four files were located in the same location as other unclassified test keys, Applicant initially believed they were unclassified, and she moved three of them to the unclassified computer. She became uncertain about the fourth file because of its subject matter and did not move it. Instead, she sent an e-mail to a more knowledgeable engineer asking about the fourth file. At the end of the work day, while in the parking lot on the way home, Applicant learned from her more knowledgeable colleague that the three files she had moved were classified. The laboratory had adopted a convention for identifying classified files by adding the letter "s" to the file name, which is a string of numbers, but the engineer who created the classified files neglected to insert an "s" in the file name. Applicant immediately returned to her work area, shut down the unclassified computer, carried it into the secure laboratory, placed a classified marker on it, and reported the incident to the security office. A security specialist verified that no back-up of the unclassified computer had been made after classified files had been moved to it. No classified information was compromised, and no formal action was taken against Applicant. This incident was the basis for the SOR ¶ 1.b.

Applicant has a reputation for being proactive in developing preventive security measures. She was a coauthor of the security plan for the laboratory. After the August 2002 security incident, Applicant suggested to her security office that the laboratory adopt additional security measures, including a double-check procedure that would require the last person to leave the laboratory to make a comprehensive security check before leaving. The procedure includes checking all safes in the laboratory to make sure they properly locked. This procedure is followed whenever the last person leaves the laboratory during the work day or at the end of the day. The only difference between a midday check and an end-of-day check is that the electronic alarm is not activated midday. The security office adopted Applicant's suggestion.

On March 17, 2003, Applicant was the last person to leave the classified laboratory at the end of the day. Earlier in the day, a colleague had closed a safe, changed the magnetic sign to reflect that it was closed, and signed the security sheet on the safe. However, he neglected to spin the dial of the lock, thereby leaving the safe unlocked. As required by the procedure she had suggested and the laboratory had adopted, Applicant checked each safe. All were closed, the outside signs read "closed," and all security sheets were signed. Applicant did not pull on the drawer, however, which would have revealed that it was not locked. She secured the laboratory door as she left. A short time later a security specialist made a spot check and discovered the unlocked safe. The specialist security secured the safe. No classified information was compromised. This incident was the basis for the SOR ¶ 1.a. The decision to revoke Applicant's security clearance was prompted by this incident but based on all three incidents.

After the March 2003 incident, Appellant held a brainstorming session with computer and security personnel to find ways to minimize the chances of a recurrence. As a result of that meeting, several additional security measures were

adopted, including reducing the number of classified computers, arranging safes in more visible positions, and using visible markers on equipment containing an encryption card. At the hearing Applicant was asked why she convened this meeting, and she responded, "It made sense. . . . I just wanted to make it less likely that violations would occur again in the future, whether it was me or someone else."

Applicant has handled and safeguarded classified materials "thousands" of times. The senior security manager for Applicant's employer regards Applicant as reliable, trustworthy, and very security conscious. The security specialist who investigated and reported all three incidents testified at the hearing and described Applicant as conscientious, dedicated, and trustworthy. Both the senior security manager and the security specialist have supported Applicant's efforts to retain her security clearance.

Applicant enjoys a reputation among her colleagues as a person of great dedication, honesty, and integrity, who is willing to take responsibility for her own actions. The three incidents were considered by her colleagues and supervisors as out of character. Her supervisors give her high marks for technical skill, organizational ability, leadership, dedication, and attention to detail. She is known as a "hands on" manager and an excellent mentor for less experienced software engineers. She has received numerous awards for superior performance. Her performance appraisal for the period following the last security incident recites, "we need a lot of Kellys."

Applicant has continued to handle a high volume of classified material since the last incident. At the time of the hearing, 19 months had elapsed without any security violations.

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.

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

In evaluating an applicant's conduct, an administrative judge should consider: (1) the nature, extent, and seriousness of the conduct; (2) the circumstances surrounding the conduct, to include knowledgeable participation; (3) the frequency and recency of the conduct; (4) the applicant's age and maturity at the time of the conduct; (5) the voluntariness of participation; (6) the presence or absence of rehabilitation and other pertinent behavioral changes; (7) the motivation for the conduct; (8) the potential for pressure, coercion, exploitation, or duress; and (9) the likelihood of continuation or recurrence. Directive ¶¶ E2.2.1.1 through E2.2.1.9.

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, that conditions exist in the personal or professional history of the applicant which disqualify, or may disqualify, the applicant from being eligible for access to classified information. *See Egan*, 484 U.S. at 531. "[T]he Directive presumes there is a nexus or rational connection between proven conduct under any of the Criteria listed therein and an applicant's security suitability." ISCR Case No. 95-0611

at 2 (App. Bd. May 2, 1996) (quoting DISCR Case No. 92-1106 (App. Bd. Oct. 7, 1993)).

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 (App. Bd. Dec. 19, 2002). "[S]ecurity clearance determinations should err, if they must, on the side of denials." *Egan*, 484 U.S. at 531; *see* Directive ¶ E2.2.2.

CONCLUSIONS

Under Guideline K, "[n]oncompliance with security regulations raises doubt about an individual's trustworthiness, willingness, and ability to safeguard classified information." Directive ¶ E2.A1.1.1. The applicable disqualifying condition in this case is DC 2: "Violations that are deliberate or multiple or due to negligence." Directive ¶ E2A11.1.2.2.

There is no evidence that any of the three incidents were deliberate, but the incidents of June 2002 (forgetting to lock the safe) and March 2003 (neglecting to double-check a colleague's safe) were negligent. Because there was more than one incident, they are "multiple." *See The American Heritage Dictionary of the English Language* (4th Ed. 2000) (defining "multiple" as "having, relating to, or consisting of more than one individual, element, part, or other component"). I conclude DC 2 is established.

The incident of August 2002 (moving a classified file onto an unclassified computer) happened in spite of Applicant's careful efforts to move only unclassified files onto the computer. The incident happened because a colleague did not follow the convention of identifying classified files by adding the letter "s" to the string of numbers in the file name. Applicant discovered the problem when she consulted with a more experienced colleague. She immediately took steps to avoid compromising the material and self-reported the incident to her security specialist. I conclude that Applicant's conduct in this incident was not negligent.

A mitigating condition (MC 1) applies if the conduct was inadvertent. Directive ¶ E2.A1.1.3.1. The unauthorized transfer of classified files to an unclassified computer despite Applicant's efforts to protect classified materials was inadvertent. I conclude MC 1 is established and the security concerns arising from the second incident (SOR ¶ 1.b.) are mitigated.

MC 2 applies if the security violations were "isolated or infrequent." Directive ¶ E2.A11.1.3.2. The first two violations occurred within two months of each other. All three violations occurred within a nine-month period. Under the circumstances, they were not "isolated or infrequent." I conclude MC 2 is not established.

MC 4 applies if an applicant has demonstrated "a positive attitude towards the discharge of security responsibilities." Directive ¶ E2.A11.1.3.4. Applicant's attitude toward her security responsibilities has been "positive" for as long as she has worked with classified materials. She coauthored the laboratory's security procedures. After her first incident when she failed to lock her safe, she was embarrassed and determined not to let it happen again. She has not had a personal security violation since March 2003.

After the second incident when she inadvertently moved a classified file onto an unclassified computer, she self-reported and took immediate action to avoid a compromise of the material. Her testimony at the hearing was notable in that she carefully avoided blaming the colleague who neglected to properly mark the classified files. Instead, she accepted responsibility for not being even more careful than she had been. After the second incident, she proactively suggested additional security precautions, including the double-check procedure that she violated in the third incident.

Applicant used the third incident as an opportunity to again review the laboratory's security procedures. As with the second incident, she accepted responsibility, did not attempt to shift blame, and used the incident as a learning experience and a catalyst for improving security procedures.

Ironically, Applicant was a victim of her own proactive approach to security. The laboratory's security specialist testified that if Applicant had not suggested the double-check procedure, it would not have been adopted, and Applicant would not have been accused of the third security violation that triggered the action to revoke her clearance.

The three incidents were qualitatively different and occurred during a nine-month period shortly after Applicant started working on classified projects. At the time, Applicant was an experienced engineer and manager but a neophyte in security procedures. The first incident (failing to secure her safe) was a personal dereliction that occurred on her first classified project, before she was accustomed to the security routine. The second (moving classified files onto an unclassified computer) was an inadvertent violation caused by a colleague's failure to adhere to the security procedure for identifying classified files. The third (failing to double-check a colleague's safe) occurred in a supervisory capacity. At the time of the hearing, nineteen months had elapsed since her last security violation.

The record amply reflects that Applicant has demonstrated a positive attitude toward security. She clearly understands that the trial-and-error approach common in software research and development, where she spent most of her career, is not acceptable in a classified environment. She has accepted responsibility for her mistakes and those of her colleagues and used them as a catalyst for improving security procedures. I conclude that MC 4 is established.

Applicant has a distinguished 20-year record. She is highly respected as a software engineer, mentor, supervisor, and civic-minded citizen. She has been aggressive in improving security procedures for her laboratory. She has handled classified materials properly thousands of times. Both the senior security officer for her employer and the security specialist for her laboratory regard her as very reliable and trustworthy, and they supported her at the hearing, one by personal testimony and one by a written recommendation.

The "whole person" concept set out in the Directive ¶ E2.2.3. contemplates that we evaluate applicants by the totality of their acts and omissions. After considering all the evidence of record, and weighing the disqualifying conditions against the mitigating conditions, I conclude Applicant has mitigated the security concern raised by her security violations. The allegations under Guideline K are resolved for Applicant.

Under Guideline E, a security concern may arise from "[c]onduct involving questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations." The conduct alleged under Guideline E is the same conduct alleged under Guideline K, discussed above. The relevant disqualifying conditions under Guideline E are DC 1 (reliable, unfavorable information provided by associates, employers, and coworkers) and DC 5 (pattern of rule violations).

The unfavorable information in this case came from the employer's security specialist and from Applicant. I conclude that DC 1 is established.

The first violation by leaving the safe unlocked and the third violation by failing to double-check a colleague's safe violated security rules. The second violation by moving the classified files to an unclassified computer was inadvertent and not Applicant's fault. Applicant violated no rules in the second incident. The first and third violations occurred nine months apart, and more than 19 months have passed without further violations. I conclude that the two rule violations do not constitute a pattern. Thus, I conclude that DC 5 is not established.

The fundamental question is whether Applicant's past conduct justifies confidence that she can be trusted to properly safeguard classified information. While Applicant's security violations cannot be condoned, her overall attitude and performance clearly establish she can be trusted to properly safeguard classified information. None of the enumerated mitigating conditions under Guideline E are applicable. However, the mitigating conditions under Guideline K are relevant, applicable to Applicant's conduct, and established by the evidence discussed above for Guideline K. Based on the entire record, I conclude the security concern raised by Applicant's personal conduct is mitigated.

FORMAL FINDINGS

The following are my findings as to each allegation in the SOR:

Paragraph 1. Guideline K (Security Violations): FOR APPLICANT

Subparagraph 1.a.: For Applicant

Subparagraph 1.b.: For Applicant

Subparagraph 1.c.: For Applicant

Paragraph 2. Guideline E (Personal Conduct): FOR APPLICANT

Subparagraph 2.a.: For Applicant

DECISION

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

LeRoy F. Foreman

Administrative Judge