DATE: August 22, 2006

In re:

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

Applicant for Security Clearance

ISCR Case No. 04-05802

DECISION OF ADMINISTRATIVE JUDGE

PHILIP S. HOWE

APPEARANCES

FOR GOVERNMENT

Julie R. Edmunds, Esq., Department Counsel

FOR APPLICANT

Pro Se

SYNOPSIS

Applicant is 44 years old, married with three children, and has worked for his defense contractor employer since 1983. Since 1997 he has had seven security violations with no compromise of classified information, all occurring in a secure location and involving forgetting to log off a computer or leaving a computer disc in the secure location. Applicant mitigated the security violations concerns. 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 13, 2005, DOHA issued a Statement of Reasons[(1)] (SOR) detailing the basis for its decision-security concerns raised under Guideline K (Security Violations) of the Directive. Applicant answered the SOR in writing on August 18, 2005 and elected to have a hearing before an administrative judge. The case was assigned to me on January 30, 2006. On February 23, 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. The Government and the Applicant submitted exhibits that were admitted into evidence. DOHA received the hearing transcript (Tr.) on March 6, 2006.

During the course of the hearing the Government moved to amend the SOR to add a seventh security violation that occurred on May 5, 2005. Applicant did not object to the amendment, and the motion was granted. Applicant admitted the allegation on the record. (Tr. 58-60)

FINDINGS OF FACT

Applicant's admissions to the SOR allegations are incorporated here as findings of fact. After a complete and thorough review of the evidence in the record, and full consideration of that evidence, I make the following additional findings of fact:

Applicant is 44 years old, married with three children, and works as a computer technician for a defense contractor. He joined his employer in 1983, and has had a security clearance since 1990. During that time his responsibilities included being custodian of the computer resource lab closed area (CRL), information security officer (ISSO) of a classified computer network in the CRL, and a backup systems administrator for various computer systems his company owned and operated. He had access to classified material from several secure lockable safes daily. He acquired these duties over time as other personnel departed the company and replacements were not hired. Applicant worked in the CRL four to eight hours daily, often up to 10 hours daily when the workload was heavy. He would enter and exit this secured area several times daily in the course of his duties. (Tr. 20-29; Exhibits A, B, C)

Applicant committed seven security violations between 1997 and 2005 during the course of his official duties for his employer. Each violation was investigated by his employer. Applicant was retrained on security protocols after each violation. Applicant also made procedural changes in his routine to prevent repeats of the individual violation types after each incident. No compromise of classified material occurred as a result of any of Applicant's actions because the violations occurred in a secured and limited access area within the employer's facility, and the facility has "security in depth" procedures. As of February 2006 his company has reduced his workload by removing and reassigning Applicant's former additional duties as main custodian for the CRL and ISSO. The company's chief security officer is confident that with these changes the possibility of future security violations by Applicant are substantially eliminated. (Tr. 20, 24, 26; Exhibits A, B, C)

Applicant first security violation occurred on December 9, 1997, when he failed to log off

a classified computer system for seven hours and two minutes. Applicant logged on to perform file transfers and departed the secret closed computer area after completing his transfers but without logging off the system. This failure was a violation of the National Industrial Security Program Operating Manual (NISPOM) Paragraph 8-304b, and paragraphs 209.10 and 4-403 of his employer's techsystems security and computer systems operating manuals, respectively. An investigation disclosed there was no compromise of classified information as a result of Applicant's actions. Applicant was retrained in proper security procedures. (Tr. 29-31, 34, 37; Exhibits 2, 8, A)

Applicant's second security violation occurred on October 29, 1998, when he forgot to log off a secure computer system in the CRL. Applicant closed the classified files upon which he was working, but forgot to log off the computer system when his work was done. There was no compromise of classified information. Applicant's actions were found by his employer to be a violation of NISPOM Paragraph 8-304b, section 109.10 of the Security Resource Manual, and Paragraph 4.503 of his employer's techsystems operating manual. Applicant was rebriefed on proper procedures. (Tr. 32-34, 47; Exhibits 3, 8, A)

Applicant's third security violation occurred on October 7, 1999, when he failed to engage the combination lock on the CRL door after he departed that room. He did not sign the log sheet on the outside of the room when he departed it. The badge reader system was engaged. The combination lock must be engaged anytime the CRL room is empty of personnel. There was no compromise of classified information as a result of Applicant's actions. His actions were investigated and found to be in violation of NISPOM Paragraph 5-306 pertaining to closed area security, and section 205-1 of the Security Resource Manual. Applicant was rebriefed on proper sign-out procedures. (Tr. 32-33, 47; Exhibits 4, 8, A)

Applicant's fourth security violation occurred on July 19, 2000, when Applicant did not properly secure a secret computer disc (CD). It was found by another employee in a computer in the CRL on July 24, 2000. Applicant forgot the CD was in the computer, took the case that originally contained it when his work with it was done, locked in a safe after following all other procedures. He did not realize the CD holder was empty. Now the CD holders are clear plastic so the user can verify the CD is in the holder. Applicant's actions were found after an investigation to be violations of NISPOM Paragraph 8-302a, section 209.24 of the Security Resources Manual, and Paragraph 4.503 of his employer's techsystems manual. No compromise of classified information occurred. Applicant was rebriefed on the proper procedures. (Tr. 34-36, 47, 52; Exhibits 5, 8, A)

Applicant's fifth security violation occurred when he left a secret tape unattended and improperly secured inside the server room of the CRL area. The tape was improperly secured for about 45 days. Applicant performed his yearly

inventory of tapes and documents. There were about 250 documents in his inventory, and he was performing the inventory shortly after taking over responsibility for the backup tapes. The room was unorganized up to that time. Six people had access to the CRL server room by badge reader at that time. Another employee found the tape on the back of one of the filing cabinets. No compromise of classified information occurred. Applicant's actions were found after a company investigation to be a violation of NISPOM Paragraph 5-306, and section 205.1 of the Security Resource Manual. Applicant was rebriefed on proper procedures when securing classified material. (Tr. 36-39, 47, 54; Exhibits 6, 8, A)

Applicant's sixth security violation occurred on May 1, 2002, when he forgot to log off the CRL computer system. The employer's investigation showed Applicant's actions to be violations of NISPOM Paragraph 8-303 and section 209.6 of the Security Resource Manual. No compromise of classified information occurred. Applicant was rebriefed on proper procedures. (Tr. 39-40,47; Exhibits 7, 8, A)

Applicant's seventh security violation was on May 5, 2005, when his workstation in the CRL was found to be logged into the computer system. No compromise of classified information occurred, in part because the log on time was only about 20 minutes. An investigation found the action to be a violation of NISPOM Paragraph 8-303, but not of the employer's security or techsystem manuals. No culpability report was submitted because Applicant was found to be merely forgetful. Corrective action was a large sign on the inside door of the CRL asking, "Did you log off?" to remind employees that they need to do that when they leave the CRL. Applicant also has a chain across his cubicle entrance to remind him to log off before he departs the CRL. He also triple checks the computers. The guard is now called when the CRL is closed after the last person departs. (Tr. 40-46; Exhibits 8, F)

At the hearing, Applicant disclosed another security violation in which he was involved in February 2005. Applicant forgot to turn on the alarm panel in the CRL when he departed that area. He noticed his mistake when he returned and notified security. The alarm for the front CRL door and the main area was not activated. The ceiling alarm was on and the door combination lock was engaged. The alarm was not engaged for about 90 minutes. An investigation ensued but no NISPOM violation was found. (Tr. 40, 41; Exhibit E)

Applicant's security officials regard him as a conscientious employee who takes his security responsibilities seriously. Applicant reported some violations himself, and recommended changes in procedures to avoid future violations. One official regards Applicant's actions as "inadvertent mistakes that occurred over time due to the high volume of activity" in which Applicant worked. They recommend Applicant retain his security clearance. (Exhibits B, C, D)

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 authorized the Secretary of Defense or his designee to grant applicants eligibility for access to classified information "only upon a finding that it is clearly consistent the national interest to do so." Exec. Or. 10865, *Safeguarding Classified Information with Industry*

§ 2 (Feb. 20, 1960). Eligibility for a security clearance is predicated upon the applicant meeting the security guidelines contained in the Directive. 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.

The adjudication process is based on the whole person concept. All available, reliable information about the person, past and present, is to be taken into account in reaching a decision as to whether a person is an acceptable security risk. Enclosure 2 of the Directive sets forth personnel security guidelines, as well as the disqualifying conditions (DC) and mitigating conditions (MC) under each guideline that must be carefully considered in making the overall common sense determination required.

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. Those assessments include: (1) the nature, extent, and seriousness of the conduct; (2) the circumstances surrounding the conduct, and the extent of knowledgeable participation; (3) how recent and

frequent the behavior was; (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 (See Directive, Section E2.2.1. of Enclosure 2). Because each security case presents its own unique facts and circumstances, it should not be assumed that the factors exhaust the realm of human experience or that the factors apply equally in every case. Moreover, although adverse information concerning a single condition may not be sufficient for an unfavorable determination, the individual may be disqualified if available information reflects a recent or recurring pattern of questionable judgment, irresponsibility, or other behavior specified in the Guidelines.

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. 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). All that is required is proof of facts and circumstances that indicate an applicant is at risk for mishandling classified information, or that an applicant does not demonstrate the high degree of judgment, reliability, or trustworthiness required of persons handling classified information. ISCR Case No. 00-0277, 2001 DOHA LEXIS 335 at **6-8 (App. Bd. 2001). Once the Government has established a *prima facie* case by substantial evidence, the burden shifts to the applicant to rebut, explain, extenuate, or mitigate the facts. *See* Directive ¶ E3.1.15. An applicant "has the ultimate burden of demonstrating that is clearly consistent with the national interest to grant or continue his security clearance. ISCR Case No. 01-20700 at 3 (App. Bd. 2002). "Any doubt as to whether access to classified information is clearly consistent with national security will be resolved in favor of the national security." Directive ¶ E2.2.2. "[S]ecurity clearance determinations should err, if they must, on the side of denials." *Egan*, 484 U.S. at 531. *See* Exec. Or. 12968 § 3.1(b).

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

Guideline K: Security Violations: *The Concern*: Noncompliance with security regulations raises doubt about an individual's trustworthiness, willingness, and ability to safeguard classified information. E2.A11.1.1

CONCLUSIONS

The Government established by substantial evidence and Applicant's admissions each of the allegations in the SOR. The Security Violations condition that could raise a security concern and may be disqualifying is Disqualifying Condition (DC) 2 (Violations that are deliberate or multiple or due to negligence. E2.A11.1.2.2). Applicant has multiple negligent violations of NISPOM and company security standards over an eight year period. They seem to occur every 10 to 12 months apart from December 1997 to May 2002, then not again until three years later in May 2005.

The applicable Mitigating Conditions (MC) are MC 1 (actions that were inadvertent. E2.A11.1.3.1) and MC 4 (Demonstrate a positive attitude towards the discharge of security responsibilities. E2.A11.1.3.4). The evidence clearly shows all these security violations were not deliberate, but were inadvertent, that is, due to Applicant's oversight and unintentional. He was performing multiple tasks for his employer in the computer area, and on a periodic occasion forgot to verify his actions or take required actions. His violations were never deliberate, but rather seemed to be cause by overwork with his multiple duties. Never was there a compromise of classified information, and all actions occurred within a secure area. His security managers submitted statements on Applicant's behalf that these were inadvertent mistakes. They consider Applicant to be a conscientious employee sincerely concerned about security.

Applicant displays a positive attitude toward his security responsibilities by his remedial actions he instituted himself, including the signs to remind him and others to log off the computer, the chain across his cubicle to remind him to take certain actions, phone calls to the guards when the last person leaves the CRL, and his rebriefs on security. He uses a clear plastic CD holder to avoid the one problem he had with thinking he had the CD in the holder and securing it, when

he left it in the computer drive. That mistake was understandable with the light weight of the CD, Applicant did not notice he was securing a CD holder in a safe without the enclosed CD. Also, he reported his actions in February 2005 when his security officer stated in his Exhibit E that it need not have been reported because other systems were in place. Finally, his employer finally recognized it was overworking Applicant with too many responsibilities, and it redistributed some of those duties to other employees, allowing Applicant to focus on his core duties and security responsibilities.

Applicant is a very credible and honest witness whose explanations of the various situations were direct and persuasive. I am especially persuaded by the statements of his two security officials and his manager that Applicant, a meticulous record keeper, is conscientitious, these violations were inadvertent,there has been no compromise of classified information at any time, and Applicant is an employee of high integrity. I conclude this security concern for Applicant.

FORMAL FINDINGS

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

Paragraph 1. Guideline K: FOR APPLICANT

Subparagraph 1.a.1: For Applicant

Subparagraph 1.a.2: For Applicant

Subparagraph 1.a.3: For Applicant

Subparagraph 1.a.4: For Applicant

Subparagraph 1.a.5: For Applicant

Subparagraph 1.a.6: For Applicant

Subparagraph 1.a.7: For Applicant

DECISION

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

Philip S. Howe

Administrative Judge

1. Pursuant to Exec. Or. 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).