

DATE: April 7, 2005

In Re:

-----

SSN: -----

Applicant for Security Clearance

ISCR Case No. 03-06569

## **DECISION OF ADMINISTRATIVE JUDGE**

**ELIZABETH M. MATCHINSKI**

### **APPEARANCES**

#### **FOR GOVERNMENT**

Daniel F. Crowley, Esq., Department Counsel

#### **FOR APPLICANT**

Francis J. Flanagan, Esq.

### **SYNOPSIS**

Aware a coworker had tampered with a door alarm that was malfunctioning in July 2002, Applicant failed to report it to his employer and was not candid during his employer's investigation of the incident. He acknowledges and regrets his poor judgment in handling of the matter, which was an aberration in his otherwise long record of compliance with security practices. Clearance is granted.

### **STATEMENT OF THE CASE**

On June 8, 2004, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) to the Applicant which 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 the Applicant. [\(1\)](#) DOHA recommended referral to an administrative judge to determine whether his clearance should be granted, continued, denied, or revoked. The SOR was based on personal conduct (Guideline E).

On June 29, 2004, Applicant, acting *pro se*, filed his response to the SOR allegations and requested a hearing before a DOHA administrative judge. The case was assigned to me on August 27, 2004. On August 30, 2004, counsel for Applicant entered his appearance. Pursuant to formal notice of September 1, 2004, a hearing was held on September 20, 2004. At the hearing, four government exhibits and two Applicant exhibits were entered into the record. Applicant, his previous supervisor (now retired), and his current supervisor testified, as reflected in a transcript received on October 4, 2004.

### **FINDINGS OF FACT**

DOHA alleges Applicant was suspended from work for one week without pay in July 2002 after he failed to report that a subordinate had tampered with an alarm at their work station, and he falsely denied any knowledge of the alarm tampering when questioned about it by his employer on July 3, and July 7, 2002. When he responded to the SOR, Applicant admitted the allegations. His admissions are accepted and incorporated as findings of fact. After a complete

and thorough review of the evidence of record, I make the following additional findings:

Applicant is a 52-year-old senior technical support engineer II who has worked for his current employer (company X), a defense contractor, since mid-May 1977. He seeks to retain a secret-level security clearance he has held since August 1977.

Applicant served on active duty in the United States military from October 1971 to November 1974. His primary specialty was telecommunications systems control specialist, and he held a top secret-level clearance with crypto access. After he had started working for his current employer, he was awarded an honorable discharge from the service in October 1977 on completion of his reserve obligation.

In the early 1980s, Applicant became supervisor of the advanced design assembly laboratory in company X's acoustics engineering department where he was responsible for coordinating and planning all technician work assignments, laboratory maintenance and safety regulations, chemical inventory and maintenance, and tooling upkeep and procurement. Very strong technically, he also proved to be very effective in dealing with his coworkers, including the five full-time technicians he supervised, the engineers and managers in other departments, as well as outside manufacturers and local machine shops. Over the February 1990 to January 1991 rating period, he took over the added responsibility for scheduling the workload of the company's test tank facility. The following year, he was given project engineering responsibilities.

During the February 1992 to February 1993 review period, he became an engineering specialist for company X, an advancement in grade, as he continued to perform his duties as supervisor of the acoustic engineering prototype assembly and test laboratory. His immediate manager was very pleased with Applicant's overall performance and commitment to the job. By February 1995, Applicant had developed a unique capability and experience base in transducer assembly and testing. His job knowledge and leadership skills were essential to the success of the laboratory, and he successfully maintained a professional working environment despite very erratic workload conditions. Applicant earned overall ratings of excellent throughout the mid to late 1990s, with promotions to senior engineering specialist in 1997 (job level 9), to senior technical support engineer I (job level A03) in mid-1998, and then to senior technical support engineer II.

As a senior technical support engineer II, Applicant continued his primary responsibility as supervisor of the acoustic engineering development laboratory and the acoustic test tank facility where he provided guidance to all of the technical support specialists while not formally evaluating their work performance. In late June 2002, an exit door in the high bay area of the laboratory, secured by a magnetic switch that would cause an alarm to ring at a security station when the door was opened, was being wired with a sound alarm audible at the door. A contractor failed to install the sound alarm properly. Left dangling by internal wires, the alarm rang at times for as long as 15 minutes, which disturbed the employees working in the area, including one technical support specialist (Mr. Y). When security guards proved to be of no help in fixing the alarm's malfunction, Mr. Y took it upon himself to silence the alarm by sealing it with some putty.

Applicant noticed the alarm had been tampered with, but he did not consider it serious as the magnetic switch, which had been in place for some 20 years, had not been deactivated so anyone wishing to exit the door still had to contact security. Applicant subsequently learned from another employee that it was Mr. Y who had sealed the alarm. Apart from confirming with Mr. Y that he had tampered with the alarm, Applicant took no action.

On July 3, 2002, company X's security manager learned from another employee the emergency exit door's local alarm had been disengaged by stuffing putty in the horn's open end. The security manager and a guard lieutenant asked both Applicant and Mr. Y if they knew who had tampered with the alarm equipment and why. Both Applicant and Mr. Y denied any involvement in the tampering or knowledge of who had tampered with the alarm. An investigation followed during which the vendor tasked with installing the alarm reported that installation was complete and the alarm was functioning properly. <sup>(2)</sup>

Applicant and Mr. Y were then interviewed that same afternoon. <sup>(3)</sup> Five to seven minutes into his interview, Mr. Y admitted he had stuffed the putty into the alarm horn, but he denied he had pulled the alarm off the wall as it had been hanging by internal wires. When Applicant was interviewed by security personnel, he stuck by his earlier story that he

did not know who deactivated the alarm or see anyone deface it, as he did not want to get Mr. Y in trouble. On further questioning, Applicant indicated he had suspicions as to the identity of the person who tampered with the alarm; that he had overheard a conversation as to who had deactivated the alarm. Applicant eventually admitted he had discussed the tampering of the alarm with the culpable technical support specialist, and finally, that he had known who had deactivated the alarm. Applicant apologized for his handling of the situation, for letting himself and security down. On his return to work after the suspension, Applicant apologized to his department manager and acknowledged that he should have handled the situation differently.

On January 14, 2003, Applicant was interviewed by a DSS special agent about his role in, and knowledge of, the tampering with the alarm. Applicant explained that the door alarm had been disturbing the employees, leading Mr. Y to stuff duct seal into it. Applicant admitted he had observed the putty in the alarm but had not seen Mr. Y place it there. Applicant also acknowledged that he had denied any knowledge of the tampering when initially questioned by company X's security personnel. Applicant admitted he had used poor judgment in not reporting the silenced alarm, in not taking security issues very seriously, and in initially lying to company X security officials when questioned.

Applicant has not been cited for any other security infractions at company X. Applicant's supervisor at company X from 1985 to late October 2001 attests to Applicant's compliance with security procedures. The manager of the acoustics department, who has known Applicant since February 1986 and has been his supervisor since April 2004, became aware of the silencing of the door alarm shortly after it occurred. While this supervisor believes Applicant made a mistake in his handling of the situation, he believes Applicant deserves to maintain his security clearance. Applicant has proven to him that he is reliable and trustworthy, including in the routine maintenance and proper functioning of classified facilities, such as the test facility where Applicant may be required to handle classified data and/or classified specifications.

## 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 with the national interest to do so." Exec. Or. 10865, *Safeguarding Classified Information within 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.

Enclosure 2 of the Directive sets forth personnel security guidelines, as well as the disqualifying conditions (DC) and mitigating conditions (MC) 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.

## CONCLUSIONS

Having considered the evidence of record in light of the appropriate legal precepts and factors, I conclude the Government established its case with respect to guideline E, personal conduct. Conduct involving questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations could indicate that the person may not properly safeguard classified information. Even after confirming that a coworker had disabled a malfunctioning security alarm at work in late June 2002, Applicant did not report the tampering to company security officials. Although access to the facility was not compromised since the magnetic switch was still operational, Applicant had an obligation as a cleared employee and as supervisor of the laboratory and test facility to report known violations of security measures. The personal conduct concerns raised by his failure to fulfill his security responsibilities are compounded by his lack of candor during his employer's investigation of the incident.

Applicant initially falsely denied to company X security officials that he had any knowledge of the silencing of the alarm. While he subsequently admitted during his July 3, 2002, interview that he was aware of the muffling of the alarm and finally of the identity of the culpable employee, it was only after repeated questioning by the investigator. Under Guideline E, disqualifying conditions E2.A5.1.2.1. *Reliable, unfavorable information provided by associates, employers, coworkers, neighbors, and other acquaintances*, and E2.A5.1.2.5. *A pattern of dishonesty or rule violations, including violation of any written or recorded agreement made between the individual and the agency*, apply.<sup>(4)</sup>

While none of the mitigating conditions under Guideline E are directly applicable, ¶ E2.2 of the Directive enumerates several factors which must be considered in evaluating an applicant's security eligibility under the whole person concept. Among these factors are the nature, extent, and seriousness of the conduct (¶ E2.2.1.1), the frequency and recency of the conduct (¶ E2.2.1.3), and the likelihood of continuation or recurrence (¶ E2.2.1.9). Applicant's failure to report a known violation of company security policy is viewed as serious, as are his false statements. However, they are not recent, and he was candid when interviewed by the DSS agent. Moreover, as confirmed by the testimonies of his former and current supervisor, Applicant has an otherwise long record of compliance with security practices at the facility. Most importantly, Applicant recognizes, and sincerely regrets, his serious lapse of judgment in not reporting the disabling of the alarm and in falsely claiming he did not know of the tampering or the identity of the culpable employee. Applicant is not likely to jeopardize his clearance or employment by engaging in similar misconduct in the future. SOR ¶ 1.a. and 1.b. are resolved in his favor.

## FORMAL FINDINGS

Formal Findings as required by Section 3. Paragraph 7 of Enclosure 1 to the Directive are hereby rendered as follows:

Paragraph 1. Guideline E: FOR THE APPLICANT

Subparagraph 1.a.: For the Applicant

Subparagraph 1.b.: For the 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 or continue a security clearance for Applicant. Clearance is granted.

**Elizabeth M. Matchinski**

**Administrative Judge**

1. The SOR was issued under the authority of Executive Order 10865 (as amended by Executive Orders 10909, 11328, and 12829) and Department of Defense Directive 5220.6 (Directive), dated January 2, 1992 (as amended by Change 4).

2. Applicant and Mr. Y's reports of the alarm's malfunction are considered more credible than the security vendor's claim that it was working properly. With the door already secured by a magnetic switch that required employees to contact security when they wanted to exit, security would not have been completely defeated by deactivating the sound alarm on the door. The nature of the action taken (stuffing putty in the horn) is consistent with Applicant's and Mr. Y's claims of alarm malfunction.

3. While the government alleged that Applicant made false statements in interviews of July 3, 2002, and July 7, 2003, the infraction report (exhibit 2) clearly indicates that Applicant as well as Mr. Y were interviewed that same afternoon. The infraction report was issued on July 2, 2002.

4. Disqualifying condition E2.A5.1.2.3. applies when a false statement concerning a relevant and material matter is made to an investigator, security official, competent medical authority, or other official representative **in connection with a personnel security or trustworthiness determination**. In other words, E2.A5.1.2.3. applies to false statements made during the investigation and/or adjudication of security clearance or suitability for access to a sensitive position. In

this case, Applicant made false statements to a security official in the investigation of a security violation at the facility and not during the personnel security investigation, so E2.A5.1.2.5. *A pattern of dishonesty or rule violations*, is more appropriate for consideration.