DATE: December 28, 2007

| | | |
|---|---|---|
| In re: | ) | |
| | ) | |
| ---------- | ) | ISCR Case No. 06-07515 |
| SSN: ---------- | ) | |
| | ) | |
| Applicant for Security Clearance | ) | |

**DECISION OF ADMINISTRATIVE JUDGE**
**PHILIP S. HOWE**

## APPEARANCES

**FOR GOVERNMENT**
Caroline H. Jeffreys, Esq., Department Counsel

**FOR APPLICANT**
Brent Harvey, Esq.

## SYNOPSIS

Applicant is 63 years old, a retired military officer, and now has 10 years experience as a corporate officer. Applicant has 40 years experience working with classified and sensitive information. He allowed his assistant without a Secret security clearance to have access to the JPAS system for 18 months, contrary to JPAS regulations, Government advisory letters, and clear guidance from his corporate security officer. Applicant failed to mitigate the handling of protected information and personal conduct security concerns. 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 June 29, 2007, DOHA issued a Statement of Reasons[1] (SOR) detailing the basis for its decision–security concerns raised under Guideline K (Handling Protected Information) and Guideline E (Personal Conduct) of the revised Adjudicative Guidelines (AG) issued on December 29, 2005, and implemented by the Department of Defense effective September 1, 2006. Applicant answered the SOR in writing on June 29, 2007, and elected to have a hearing before an administrative judge. The case was assigned to me on October 25, 2007. On November 14, 2007, 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 November 28, 2007.

## 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 63 years old, married, and has adult children. He served 30 years in the U.S. Air Force, retiring in the grade of Colonel. After retirement, he started work for a defense contractor as the office manager of its local office, and now as a Vice-President of the company. He also acts as its local facility security officer (FSO), and had that duty for 10 years. He spends about 10% of his business day on FSO duties. (Tr. 69, 70, 87, 90; Exhibits 1, A-C)

Applicant has a reputation as being trustworthy and honest. His character statements by colleagues and friends show that they consider him as a man of integrity, professionalism, sound judgment, and competency. Applicant had many years of experience in the Air Force with classified programs, security programs, and handling classified information. (Tr. 122-145; Exhibits A-C)

Applicant hired another retired officer in 2001 to assist him in his FSO duties. That person applied for a security clearance, but was denied in March 2003. Applicant testified at a hearing as a character witness for that person, and wrote a letter in November 2002, on behalf of that person. That person has reapplied for a security clearance, and his application is pending with the Government. Applicant retained that person in his office and on the company payroll in a part-time position. That person had access to information in the Joint Personnel Adjudication System (JPAS) in its original paper document configuration, and then from 2004 to 2005 on the computer-based system. Only persons with a security clearance are permitted to have access to JPAS. (Tr. 52-54, 84, 92, 96, 97, 109, 111, 115, 117, 118, 120; Exhibits 5-11)

[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).

The JPAS system became the system of record for contractors in the Department of Defense on October 1, 2004. The Industrial Security Letter of July 15, 2004, explained the new requirements for access to JPAS by FSO personnel and anyone else authorized access. A Secret clearance or an "eligibility" determination based on a favorably adjudicated investigation is now required for access to JPAS. The information in JPAS is not classified, but privacy protected. FSO's have a higher level of access for their duties than other persons. JPAS training sessions were listed on-line for enrollment purposes by a government agency. Contractors were made responsible for getting their employees trained on JPAS. The JPAS system is a DoD computer system, subject to the Privacy Act of 1974. The system is also subject to the National Industrial Security Program Operating Manual (NISPOM), paragraph 2-200b, and the written procedures from the Defense Security Service (DSS) dated April 2007. (Exhibits 8-13)

Applicant's company got access to JPAS in April 2004. The corporate security officer in its headquarters gave all company FSO's, including Applicant, a user name and password in a telephone call made to each person in March 2004. That official received the user names and passwords from the DSS. Applicant was personally responsible under his company's policy for JPAS at his work location. Applicant was notified in a memorandum dated March 12, 2004, from company headquarters that his uncleared assistant could not have access to JPAS. On July 15, 2005, that uncleared employee sent an email to the company's corporate security officer complimenting a company employee for her help in getting him operational on the JPAS system, to which he was not authorized access. On July 27, 2005, that officer notified DSS that Applicant allowed the uncleared employee assistant access to JPAS, even though he did not have a Secret security clearance, by allowing the employee to access JPAS through Applicant's account. Applicant gave the employee his user name and password. The employee also assisted Applicant in the periodic changes of Applicant's password. In July 2005, Applicant changed his procedures by moving the JPAS computer into his office and denying his assistant access to the computer, but continued to give him information from the JPAS system in paper print-out format. Applicant told a Government investigator in April 2006, that he was unaware that JPAS regulations required an appropriate security clearance to have access to JPAS. (Tr. 22-45, 47-62, 72-77, 92-97; Exhibits 2-4, 14)

Applicant claims he did recall receiving the Industrial Security Letters, NISPOM procedures, and the emailed memorandum of March 12, 2004, from his company's corporate security office, or reading them. He knew he received them periodically. Applicant had access to his email system and the record on that system shows he opened the email. DSS sent the Industrial Security Letters by mail to each FSO and later electronically notified each FSO that the letters were available on line for reading. Applicant was aware that JPAS was being implemented in 2004. His office got access in August 2004. After a meeting in September 2005 with a senior industrial security specialist from DSS about the uncleared employee having JPAS access, Applicant changed his password so the employee did not have it. Applicant did not comprehend any difference in the prior paper-based system and the new JPAS system, so he did not think there was any problem with allowing his uncleared subordinate access to the JPAS through Applicant's account. (Tr. 47-57, 74-84, 98, 101-107, 113; Exhibits 2-4, 8-13)

Applicant received local training on JPAS, and did not use the government training programs. Nor did he attend any company-sponsored training programs. The corporate security officer and his assistant attended such a program in 2004. (Tr. 24, 81, 112; Exhibits 8-13)

## 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: The Concern: Deliberate or negligent failure to comply with rules and regulations for protecting classified or other sensitive information raises doubt about an individual's trustworthiness, judgment, reliability, or unwillingness and ability to safeguard such information, and is a serious security concern. ¶ 33

Guideline E: Personal Conduct: The Concern: Conduct involving questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations can raise questions about an individual's reliability, trustworthiness and ability to protect classified information. Of special interest is any failure to provide truthful and candid answers during the security clearance process or any other failure to cooperate with the security clearance process. ¶ 15

## CONCLUSIONS

**Guideline K:** Applicant denied the allegation under this Guideline. However, Applicant had 30 years experience in the Air Force working on classified programs and complying with security regulations. He had 10 years of private sector experience as the FSO for his work location. Applicant knew the JPAS was being implemented in 2004, and received a new user name and password by his corporate security officer in March 2004. The corporate security officer's senior security coordinator on March 12, 2004, told Applicant his designated assistant was not a cleared person, and consequently, could not have access to JPAS.

Yet, Applicant continued to allow that assistant access to the JPAS system between March 2004 and June 2005. Applicant gave the employee his user name and password, allowed him to enter the JPAS system using the passwords, and perform functions on JPAS that the employee, without a Secret clearance, was not authorized to do. That situation directly contravened the requirements of the JPAS accessibility system.

Applicant knew the employee did not have a Secret clearance because he wrote a character letter for him in 2002, and testified for him at his security clearance hearing in 2003. Applicant knew the employee was denied a security clearance in March 2003.

Based on 40 years experience in government security requirements, Applicant knew or should have known of the new JPAS accessibility requirements. Even after being told his assistant could not have access to JPAS, Applicant ignored that advice and the requirements set forth in the Industrial Security Letters, and other written documents discussing JPAS.

The applicable Disqualifying Conditions (DC) are ¶ 34 (a) (deliberate or negligent disclosure of classified or other protected information to unauthorized persons, including but not limited to personal or business contacts, to the media, or to persons present at seminars, meetings, or conferences), and ¶ 34 (g) (any failure to comply with rules for the protection of classified or other sensitive information).

I considered were all three Mitigating Conditions (MC) under ¶ 35. Two years has elapsed since the last violation in September 2005, but the duration of the violations, from March 2004 to September 2005, outweigh that passage of time. The violations did not happen infrequently, but rather daily or weekly for that 18 month period. There were no unusual circumstances involved, because Applicant knew he was acting contrary to the JPAS requirements. Applicant as the local manager could have designated another person who had a Secret clearance to be his assistant. While the situation is now unlikely to recur, the sequence of events, when compared to Applicant's experience in this area, casts doubt on his current reliability, trustworthiness, and good judgment because he persisted in his conduct after being told not to designate the uncleared person as his assistant. Therefore, MC ¶ 35 (a) does not apply. While Applicant has a positive attitude toward his security responsibilities, he was not a beginner in security compliance, but was the manager and FSO. He refused to comply with JPAS requirements even after being told in March 2004, that he was acting incorrectly. MC ¶ 35 (b) does not apply. Lastly, ¶ 35 (c) does not apply because training was available, and as a manager he had the duty to obtain it. Applicant has 40 years experience in compliance with security requirements. He is not a new and inexperienced employee, and had a duty to comply with JPAS requirements from the start of the program.

**Guideline E:** Applicant denied these allegations under this guideline. While he told the Government investigator he was unaware of the JPAS security clearance requirements when the system became operational, Applicant received an email inquiry and notification on March 12, 2004, from his company's senior security coordinator that his assistant had no security clearance and could not have access to JPAS. Applicant was on notice from March 2004 onward that his assistant was not cleared for access to JPAS, but apparently chose to ignore it.

Two DC under this Guideline apply: ¶ 16 (c) (credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any single guideline, but which, when considered as a whole, supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the person may not safeguard protected information); and, ¶ 16 (d) (credible adverse information that is not explicitly covered under any other guideline and may not be sufficient by itself for an adverse determination, but which, when combined with all available information supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating the person may not properly safeguard protected information. This includes but is not limited to consideration of (1) untrustworthy or unreliable behavior to include breach of client confidentiality, release of proprietary information, unauthorized

release of sensitive corporate or other protected information; (3) a pattern of dishonesty or rule violations). Applicant knew for 18 months he should not have allowed his assistant to have access to JPAS, but persisted in that conduct. When his company superiors discovered the violation, they reported it, and finally Applicant took corrective action to change his password in September 2005 after meeting with a Government industrial security representative.

Examining and considering the MC under this guideline, none of the subsections under ¶ 17 apply. Applicant was confronted with the facts and then took action, so ¶ 17(a) does not apply. ¶17 (b, d-g) are not applicable on the facts. ¶ 17 (c) might apply if the situation were minor, but Applicant allowed a major violation of JPAS requirements for 18 months, knowing that his assistant was not qualified to have access, and only changed the process after being confronted with the facts and the regulations.

**Whole Person Analysis**

"The adjudicative process is an examination of a sufficient period of a person's life to make an affirmative determination that the person is eligible for a security clearance." AG ¶ 2(a). "Each security clearance decision must be a fair and impartial common sense determination based upon consideration of all the relevant and material information and the pertinent criteria and adjudication policy." Directive ¶ 6.3. "Available, reliable information about the person, past and present, favorable and unfavorable, should be considered in reaching a determination." AG ¶ 2(a). In evaluating Applicant's case, I have considered the adjudicative process factors listed in the AG ¶ 2(a).

Of those factors, ¶ 2 (1-5, 7-9) apply to the facts. Applicant is an experienced military and corporate officer with decades of security training and experience. He was told in March 2004 his designation of an uncleared assistant for access to JPAS was wrong, but he persisted. He failed to educate himself more thoroughly if he had any questions about the accessability requirements. His conduct persisted for 18 months until Government officials and corporate officials confronted him. He voluntarily allowed his assistant access, in part because he trusted him, hired him into the company, and found his work satisfactory. The problem was that the assistant had been denied a security clearance in March 2003, and Applicant knew of that denial. Applicant found it convenient to have his assistant do the JPAS work because of Applicant's other corporate duties required much of his time. Under such circumstances, Applicant should have hired or assigned another assistant, or relinquished the FSO duties. There is a potential for coercion in the future based on this pattern of conduct, and a likelihood of recurrence because of Applicant's prior lack of attention to the JPAS requirements.

Therefore, I conclude the Handling of Protected Information security concern against Applicant. I conclude the Personal Conduct security concern against Applicant. Finally, I conclude the "whole person" concept against Applicant.

## FORMAL FINDINGS

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

| | |
|---|---|
| Paragraph 1. Guideline K: | AGAINST APPLICANT |
| Subparagraph 1.a: | Against Applicant |
| Paragraph 2. Guideline E: | AGAINST APPLICANT |
| Subparagraph 2.a.1: | Against Applicant |
| Subparagraph 2.a.2: | Against 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.

Philip S. Howe
Administrative Judge