DATE: March 7, 2001

In Re:

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

Applicant for Security Clearance

ISCR Case No. 00-0291

DECISION OF ADMINISTRATIVE JUDGE

ROBERT ROBINSON GALES

APPEARANCES

FOR GOVERNMENT

Martin H. Mogul, Esquire, Department Counsel

FOR APPLICANT

Douglas G. Andrews, Esquire

SYNOPSIS

Thirty-eight year old Applicant's pattern of employer rule violations pertaining to the confidentiality and privacy of sensitive hospital patient information by wrongfully accessing computer files; his subsequent discharge for those actions; and the current absence of credible evidence of rehabilitation, raise grave questions and doubts as to his security eligibility and suitability. Clearance is denied.

STATEMENT OF THE CASE

On October 17, 2000, the Defense Office of Hearings and Appeals (DOHA), 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, issued a Statement of Reasons (SOR) to 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 Applicant, and recommended referral to an Administrative Judge to determine whether a clearance should be granted, continued, denied, or revoked.

In a sworn written statement, undated, Applicant responded to the allegations set forth in the SOR, and requested a hearing. The case was initially assigned to Administrative Judge John G. Metz, Jr., on December 7, 2000 but, due to caseload considerations, was subsequently reassigned to, and received by, this Administrative Judge on December 26, 2000. A notice of hearing was issued on December 29, 2000, and the hearing was held before me on January 25, 2001. During the course of the hearing, four Government exhibits and six Applicant exhibits, and the testimony of three Applicant witnesses (including Applicant), were received. The transcript (Tr.) was received on February 13, 2001.

FINDINGS OF FACT

Applicant has admitted the sole factual allegation pertaining to personal conduct under Guideline E. That admission is incorporated herein as a finding of fact.

After a complete and thorough review of the evidence in the record, and upon due consideration of same, I make the following additional findings of fact:

Applicant is a 38 year old male employed by a defense contractor, and he is seeking to obtain a security clearance, the level of which has not been described.

Applicant had previously been employed as a safety and security officer of a particular hospital from June 1989 until October 1997.[(1)] He was 26 years of age at the time he commenced his employment. At some point during that period, thought by Applicant to be during 1996-97,[(2)] a new computer system was installed in the hospital and Applicant was furnished with a key and password to access the system.[(3)] He was furnished with little, if any, instruction regarding computer use.

On at least three[(4)] different occasions during his period of employment, Applicant was furnished varying degrees of training regarding the confidentiality of medical information. In June 1989, he signed an Employee Confidentiality Statement[(5)] in which he stated he understood and agreed that in the performance of his duties as an employee of the hospital he "must hold medical information in confidence." In August 1995, Applicant signed a Certification in which he stated he had received and "thoroughly reviewed" the Corporate Compliance Plan.[(6)] The Corporate Compliance Manual contained the following language:[(7)]

Except as specifically authorized by the patient or by [employer hospital's] policies, no [employer hospital] employee shall:

- Obtain medical information from a patient's record or from another employee if the employee obtaining the information does not need to know the information for purposes of providing care, performing medical quality review, submitting claims for reimbursement, or other authorized and appropriate purposes.

  In May 1997, he signed another such statement[(8)] in which he stated he understood and agreed that in the performance of his duties as an employee of the hospital he "must hold medical, financial and personnel information in confidence."

  Despite having read the hospital policy on confidentiality, in late 1996 or early 1997,[(9)] over the course of at least two or three months,[(10)] Applicant accessed patient records in the system on an estimated 10 to 20 occasions.[(11)] In so doing, he pulled up the names of people whom he knew had their records on the system and viewed their files.[(12)] During this period, Applicant mentioned his computer system activities to a couple of people but never gave the matter much thought. Finally, in about October 1997, Applicant's supervisor became aware of Applicant's activities after a female employee reported that Applicant had viewed her medical file.[(13)] The supervisor approached Applicant regarding the alleged violation of hospital policy. The matter was reported to Human Resources. Applicant acknowledged "there was no professional or work related reason" for him to have access to the computer system.[(14)]

  On October 29, 1997, Applicant was discharged from further employment for violation of the established hospital policy pertaining to confidentiality of patient information.[(15)] Applicant's subsequent request for reinstatement was denied.

  Applicant's explanations for accessing the sensitive hospital patient information were as follows: (1) since he worked mostly nights and did not have tasks to perform, he started to "mess" with the computers to improve his "computer knowledge;"[(16)] (2) he simply wanted to experiment with the computer and find out what he could do with it;[(17)] and (3) he wanted to improve his computer skills.[(18)] At the time of his computer activities, Applicant did not consider such actions to be a violation of hospital policy.[(19)] Applicant expressed regret over the policy violations and attributed his actions to ignorance and a lack of understanding, as well as, in retrospect, stupidity.

(20) He also defended his actions by claiming that none of the accessed computer information was ever written down, printed, or otherwise disseminated to third parties.(21)

After his termination in October 1997, Applicant underwent a brief period of unemployment before securing his present security position with a government contractor. Present and former co-workers and supervisors have favorably characterized his character and performance, using the following descriptions: personable, courteous, professional, dedicated, honest, trustworthy, and dependable. He has generally met or exceeded the performance standards of his current and past positions.

POLICIES

Enclosure 2 of the Directive sets forth adjudicative guidelines which must be considered in the evaluation of security suitability. In addition to brief introductory explanations for each guideline, the adjudicative guidelines are divided into those that may be considered in deciding whether to deny or revoke an individual's eligibility for access to classified information (Disqualifying Conditions) and those that may be considered in deciding whether to grant an individual's eligibility for access to classified information (Mitigating Conditions).

An Administrative Judge need not view the adjudicative guidelines as inflexible ironclad rules of law. Instead, acknowledging the complexities of human behavior, these guidelines, when applied in conjunction with the factors set forth in the Adjudicative Process provision set forth in Section E2.2., Enclosure 2, of the Directive, are intended to assist the Administrative Judge in reaching fair and impartial common sense decisions.

Because the entire process is a conscientious scrutiny of a number of variables known as the "whole person concept," all available, reliable information about the person, past and present, favorable and unfavorable, should be considered in making a meaningful decision. The Adjudicative Process factors which an Administrative Judge should consider are: (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.

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:

[Personal Conduct - Guideline E]: 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.

Conditions that could raise a security concern and may be disqualifying also include:

(1) Reliable, unfavorable information provided by associates, employers, coworkers, neighbors, and other acquaintances;

(5) A pattern of dishonesty or rule violations, including violation of any written or recorded agreement made between the individual and the agency.

Conditions that could mitigate security concerns include:

None apply.

Since the protection of the national security is the paramount consideration, the final decision in each case must be arrived at by applying the standard that the issuance of the clearance is "clearly consistent with the interests of national security,"(22) or "clearly consistent with the national interest." For the purposes herein, despite the different language in each, I have concluded that both standards are one and the same. In reaching this Decision, I

have endeavored to draw only those conclusions that are reasonable, logical and based on the evidence contained in the record. Likewise, I have attempted to avoid drawing inferences that are grounded on mere speculation or conjecture.

In the decision-making process, the burden of producing evidence initially falls on the Government to establish a case which demonstrates, in accordance with the Directive, it is not clearly consistent with the national interest to grant or continue an applicant's access to classified information. If the Government meets its burden, the heavy burden of persuasion then falls upon the applicant to present evidence in refutation, explanation, extenuation or mitigation sufficient to overcome the doubts raised by the Government's case, and to ultimately demonstrate it is clearly consistent with the national interest to grant or continue the applicant's clearance.

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 that 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 that 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.

One additional comment is worthy of note. Applicant's allegiance, loyalty, and patriotism are not at issue in these proceedings. Section 7 of Executive Order 10865 specifically provides that 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 I have based this decision, in whole or in part, on any express or implied decision as to Applicant's allegiance, loyalty, or patriotism.

CONCLUSIONS

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

With respect to Guideline E, the Government has established its case. Examination of Applicant's actions reveals a pattern of conduct involving questionable judgment, untrustworthiness, and unreliability. There is little dispute surrounding Applicant's actions for he has admitted the essential elements of the repeated violations and been disciplined--and discharged--for them. Applicant accepted fiduciary responsibilities as a hospital safety and security officer, and was intrusted with keys and passwords to gain access to areas and computers, as necessary in the proper undertaking of his professional responsibilities. Furthermore, on four separate occasions, he acknowledged he understood and agreed that in the performance of his duties as an employee of the hospital he would hold medical, financial and personnel information in confidence, consistent with the hospital policy on confidentiality. Nevertheless, Applicant repeatedly disregarded those known policy and procedures by wrongfully accessing sensitive medical information on the hospital computer system. Applicant's overall questionable personal conduct in this regard clearly falls within Personal Conduct Disqualifying Condition (DC) E2.A5.1.2.1. and DC E2.A5.1.2.5., cited above.

While this matter is not alleged under Guideline M, Misuse of Information Technology Systems, I believe a brief discussion of that guideline under the facts herein could be constructive. The stated concern under that guideline is, in part: "Noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual's trustworthiness, willingness and ability to properly protect classified systems, networks, and information." One such condition that could raise a security concern and may be disqualifying is: (1) Illegal or unauthorized entry into any information technology system. Conditions that could mitigate security concerns include: (1) The misuse was not recent or significant; (2) The conduct was unintentional or inadvertent; and (4) The misuse was an isolated event.

While the subject computer system involved only sensitive information and not classified information, the concern is identical. Applicant's repeated access to the system information may not have been "illegal," but it certainly was both unauthorized and in violation of established policy. The potential mitigating conditions under this guideline do not apply. It might conceivably be argued that Applicant's conduct was not "recent." However, the term is not defined in the Executive Order, Regulation, or the Directive, and could, depending on differing circumstances, have various interpretations. In this instance, I conclude that Applicant's 1996-97 conduct was, in relative terms, "recent"--too recent to overlook. The policy violations were significant enough to warrant Applicant's immediate termination by his employer. The conduct was routine over a period of months and cannot be considered an isolated event. And finally, the conduct by Applicant's admissions was intentional: he started to "mess" with the computers to improve his computer knowledge and accessed sensitive computer information in an attempt to improve his computer skills. Had Guideline M been alleged, Applicant's overall misuse of information technology systems in this regard would clearly fall within DC E2.A13.1.2.

A person should not be held forever accountable for misconduct from the past. However, without a clear indication of subsequent reform, remorse, or rehabilitation, I am unable to determine with reasonable certainty the probability that such conduct will not recur in the future. In this instance, Applicant has offered a variety of explanations for using knowledge, keys, and passwords intrusted to him for safekeeping and utilization under the appropriate circumstances. He eventually expressed regret over the policy violations and attributed his actions to ignorance and a lack of understanding, as well as, in retrospect, stupidity. But he still seeks to exonerate his actions by claiming they did not result in the disclosure of sensitive information to others. Aside from his brief acknowledgment that he had acted stupidly in 1996-97, the record is silent as to any indicia of rehabilitation and other positive behavioral changes.

I do not take this position lightly, but based on the law, as set forth in *Department of Navy v. Egan,* 484 U.S. 518 (1988), my evaluation of the evidence, and my application of the pertinent factors and conditions under the Adjudicative Process, I believe Applicant has failed to mitigate or overcome the Government's case. The evidence leaves me with grave questions and doubts as to Applicant's continued security eligibility and suitability. Accordingly, allegation 1.a. of the SOR is concluded against Applicant.

For the reasons stated, 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 E: AGAINST THE APPLICANT

Subparagraph 1.a.: Against the 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.

_____

Robert Robinson Gales

Chief Administrative Judge

1. *See*, Government Exhibit 1 (Security Clearance Application, Standard Form 86, dated March 18, 1999), at 2.

2. *See*, Tr., at 40, 47.

3. *Id.,* at 48.

4. There is a reference to a fourth such certificate, supposedly completed in June 1996, mentioned in Applicant Exhibit F (Report of Investigation, undated), but no such certificate was offered into evidence. Nevertheless, because the exhibit was offered by Applicant, I have concluded that there were four such certifications.

5. *See*, Government Exhibit 3 (Employee Personnel File), at 6.

6. *Id.,* at 5.

7. *Id.,* at 4.

8. *Id.,* at 7.

9. *See*, Tr. at 40.

10. *Id.*, at 41.

11. *Ibid.*

12. *See*, Government Exhibit 2 (Statement of Subject, dated September 28, 1999), at 1-2.

13. *See* Applicant Exhibit F, *supra* note 4, at 2.

14. *See*, Government Exhibit 3 (Employee Comments attached to Disciplinary Action Report, dated October 29, 1997), *supra* note 5, at 21.

15. *Id.*, Government Exhibit 3 (Separation Notice, dated October 29, 1997), at 15.

16. *See*, Government Exhibit 2, *supra* note 12, at 1.

17. *See*, Government Exhibit 3 (Employee Comments attached to Disciplinary Action Report, dated October 29, 1997), *supra* note 5, at 20.

18. *See*, Tr. at 43.

19. *See*, Government Exhibit 2, *supra* note 12, at 2.

20. *See*, Response to SOR, undated, at 2.

21. *See*, Tr. at 29-30.

22. *See*, Executive Order 12968, *"Access to Classified Information;"* as implemented by Department of Defense Regulation 5200.2-R, *"Personnel Security Program,"* dated January 1987, as amended by Change 3, dated November 8, 1995, and further modified by memorandum, dated November 10, 1998. However, the Directive, as amended by Change 4, dated April 20, 1999, uses both "clearly consistent with the national interest" (*see*, Sec. 2.3.; Sec.2.5.3.; Sec. 3.2.; and Sec. 4.2.; Enclosure 3, Sec. E3.1.1.; Sec. E3.1.2.; Sec. E3.1.25.; Sec. E3.1.26.; and Sec. E3.1.27.), and "clearly consistent with the interests of national security" (*see*, Enclosure 2, Sec. E2.2.3.); and "clearly consistent with national security" (*see*, Enclosure 2, Sec. E2.2.2.)