DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
----------	)	ISCR Case No. 07-02689
SSN: ----------	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Robert E. Coacher, Esquire, Department Counsel
For Applicant: *Pro se*

September 9, 2008

Decision

GALES, Robert Robinson, Chief Administrative Judge:

Applicant mitigated the security concerns regarding handling protected information and personal conduct. Eligibility for a security clearance and access to classified information is granted.

Statement of the Case

On November 3, 2005, Applicant applied for a security clearance and submitted an ESPQ version of a Security Clearance Application (SF 86). On November 8, 2007, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) to him, pursuant to Executive Order 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended and modified; and Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended and modified (Directive). The SOR alleged security concerns under Guideline K (Handling Protected Information) and Guideline E (Personal Conduct), and detailed reasons why DOHA could not make a 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.

On December 29, 2005, the President promulgated revised *Adjudicative Guidelines for Determining Eligibility For Access to Classified Information*, and on August 30, 2006, the Under Secretary of Defense (Intelligence) published a memorandum directing implementation of those revised Adjudicative Guidelines (AG) for all adjudications and other determinations made under the Directive and Department of Defense (DoD) Regulation 5200.2-R, *Personnel Security Program* (January 1987), as amended and modified (Regulation), in which the SOR was issued on or after September 1, 2006. The AG applies to Applicant's case because his SOR was issued after September 1, 2006.

Applicant received the SOR on November 25, 2007. In a sworn, written statement, dated November 26, 2007, Applicant responded to the SOR allegations and requested a hearing before an Administrative Judge. Department Counsel indicated the Government was prepared to proceed on April 8, 2008, and the case was assigned to me on April 11, 2008. A Notice of Hearing was issued that same day, and I convened the hearing, as scheduled, on May 8, 2008.

During the hearing, three Government exhibits and three Applicant exhibits were received and admitted, some over objection. Applicant testified. The transcript of the hearing (Tr.) was received on May 16, 2008.

Findings of Fact

In his Answer to the SOR, Applicant admitted most of the factual allegations (¶¶ 1.b., 1.c., and 2.a.) of the SOR with explanations, and denied the remaining allegations.

Applicant is a 27-year-old employee of a defense contractor, and he is seeking to retain a SECRET security clearance. He has been employed as an integration and test engineer by the same government contractor since July 2005.[1] Prior to his current employment he was on active duty with the U.S. Navy from August 1999 until June 2004, and honorably discharged as a Petty Officer 2nd Class (E-5)[2]; a field engineer with another defense contractor from June 2004 until April 2005; and unemployed from April 2005 until July 2005.[3]

There are two differing scenarios regarding an incident that transpired on March 23, 2005, which is the sole focus of the SOR. The first scenario, described below, is that of the Applicant, and is supported by his Answer to SOR and testimony; the second

[1] Government Exhibit 1 (Security Clearance Application, dated Nov. 3, 2005), at 2.

[2] *Id.* at 3-4

[3] *Id.* at 2.

one, from the then-employer, supported by an Adverse Information Report, is described thereafter.

On March 23, 2005, Applicant was offered a job from a competing defense contractor program manager which would have increased his then-current salary by $20,000.00.[4] Applicant informed his then-current program manager (PM) and asked if his employer could match the offer. His PM was apparently "furious" at the competitor because he had already lost another employee to them.[5]

That same evening, at about 10:30 p.m., after having dinner, Applicant and a female companion (who was a cleared employee working for the same Command at another location)[6] entered the closed military facility after passing two checkpoints, including a gate guard who touched Applicant's badge. Their original purpose for being on the facility at that time was for her to drop Applicant off for work and then borrow his automobile.[7] Instead, they drove around the perimeter of the base and parked for a scenic view overlooking the ocean.[8] Applicant's companion said she needed to use the restroom so they drove to the unsecured building where he worked, entered it, and he escorted her to the restroom which was outside of the secured laboratory.[9] He never took, or attempted to take, her into the laboratory itself.[10] Applicant called to a colleague to meet her in the hallway. Shortly thereafter, they departed the area and drove back to the restaurant to pick up her car.[11]

Applicant had worked his shift from 10 p.m. the previous day until 6 a.m. that day. The established policy was to have flexible hours if anyone worked overtime earlier in the week, and it was noted on the time card.[12] Applicant did not work the entire period he was scheduled to do so.[13]

The following day, a security stand down day,[14] his PM informed Applicant that his employer could offer him a salary increase, but because the amount did not match

[4] Tr. at 48.

[5] Answer to SOR, dated Nov. 26, 2007, at 1.

[6] Tr. at 33.

[7] *Id.* at 34.

[8] *Id.*

[9] *Id.* at 34-35, 37.

[10] *Id.* at 35-36.

[11] Answer to SOR, *supra* note 5, at 2-3.

[12] Tr. at 30.

[13] *Id.* at 39.

[14] *Id.* at 57.

the competitor's offer, Applicant stated he was still undecided as to what his decision would be.[15]

On March 29, 2005, Applicant's PM called regarding the decision, and Applicant told him he decided to submit his two week notice. The PM told him to type his letter of resignation stating his last day of work, and Applicant did so.[16] He also commented about the "incident" of March 23rd and added that if Applicant could keep the next two weeks clean, he would have his "going-away" party the next week. Two hours later, Applicant was told he was being placed on administrative leave until the "incident" could be resolved. That evening, the PM came to Applicant's apartment and requested statements from Applicant and his female friend and picked up Applicant's badge.[17] The statements were e-mailed as requested.[18]

The following day, the PM called Applicant and asked to meet him as the security office. Applicant was questioned by an investigator and subsequently advised by the PM that ". . . hopefully they just revoke access for 6 months and you can continue your career and we can still be friends."[19] The end result was that Applicant was terminated from his job, effective March 31, 2005.[20] Although Applicant had anticipated commencing employment with his new employer on April 18, 2005,[21] because he was now barred from the facility, the offer was withdrawn.[22]

The scenario offered by the then-employer Facility Security Officer is markedly different from that described above.

On March 23, 2005, at some time between 10:30 p.m. and 12:00 a.m., Applicant "knowingly and willfully snuck an unauthorized girlfriend onto the . . . Naval Base and attempted to bring her into a classified lab. . . . Another employee stopped [Applicant] from bringing his guest into the classified lab and told him to get her off of the base."[23]

The issue of the falsified timecard was described as follows:

---

[15] Answer to SOR, *supra* note 5, at 1.

[16] Tr. at 53-55.

[17] *Id.* at 64.

[18] Answer to SOR, *supra* note 5, at 2.

[19] *Id.*

[20] Tr. at 38, 65.

[21] *Id*. at 60.

[22] *Id*. at 67.

[23] Government Exhibit 2 (Adverse Information Report, dated Apr. 5, 2005).

> . . . He then left the base but did not return until approximately 3:00 a.m. It was further uncovered that [Applicant] falsified his timecard given that he reported he worked the hours of 9:30 p.m. to 6:00 a.m. but was off the base from approximately 9:30 p.m. to 3:00 a.m.[24]

Applicant's candor was characterized as follows:

> . . . His version of the events has also changed several times and what we were told by [Applicant] is slightly different than what he told the . . . base investigators.[25]

As of April 5, 2005, the incident had been reported to the Command security office and "is currently under investigation"[26], and Applicant's access privileges to the base and lab were temporarily revoked until further notice. Applicant was put on administrative leave immediately so that the then-employer might investigate the incident.[27] Nevertheless, with the understanding that Applicant had previously given notice of his intent to terminate his employment on March 29, 2005, it was decided that he should be terminated, effective March 31, 2005, because the investigation of the incident was apparently completed and something unspecified was "uncovered."[28]

While Applicant's scenario contained some uncertainty regarding the specific dates certain actions occurred, his explanation has the ring of truth. On the other hand, while it appears the then-employer, as well as the Command security office, had conducted an inquiry or investigation of the incident which occurred on March 23, 2005, no such reports of inquiry or investigation, along with interview statements of Applicant and witnesses, have been submitted. Instead, there are findings, conclusions, and characterizations unsupported by specifics other than what was alleged in the Adverse Information Report.

For example, the report stated Applicant "willfully snuck an unauthorized girlfriend" onto the base and "attempted to bring her into a classified lab" but was stopped by another employee. There is nothing in evidence as to how he "willfully snuck" someone on base, or how he "attempted" to bring her into the classified lab, or who, and under what circumstances, the unidentified employee stopped him. In addition, it is alleged that his version of the events changed several times, but there is no explanation as to what his versions were or how they differed. Under the circumstances, considering the conflicting interpretations of the actions and the incident, as well as the very sparse evidence presented by the Government, I accept Applicant's explanations rather than the Government's unsupported interpretations of same.

---

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] *Id.*

Since becoming employed by his current employer, Applicant was closely monitored by the Facility Security Officer because of the earlier incident with his former employer. After 18 months of "stellar security performance," Applicant was selected and trained to be COMSEC Custodian, a position he handled with "superior results."[29] He has also been recognized by the Commander, USCENTAF, and his Program Manager for his contributions to the mission.[30]

Policies

When evaluating an Applicant's suitability for a security clearance, the Administrative Judge must consider the revised Adjudicative Guidelines. In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially disqualifying conditions and mitigating conditions, which are useful in evaluating an Applicant's eligibility for access to classified information.

An Administrative Judge need not view the guidelines as inflexible, ironclad rules of law. Instead, acknowledging the complexities of human behavior, these guidelines are applied in conjunction with the factors listed in the adjudicative process. The Administrative Judge's over-arching adjudicative goal is a fair, impartial and common sense decision. According to AG ¶ 2(c), the entire process is a conscientious scrutiny of a number of variables known as the "whole person concept." The Administrative Judge must consider all available, reliable information about the person, past and present, favorable and unfavorable, in making a meaningful decision.

Since the protection of the national security is the paramount consideration, AG ¶ 2(b) requires that "[a]ny doubt concerning personnel being considered for access to classified information will be resolved in favor of national security." In reaching this decision, I have drawn only those conclusions that are reasonable, logical and based on the evidence contained in the record. Likewise, I have avoided drawing inferences grounded on mere speculation or conjecture.

In the decision-making process, facts must be established by "substantial evidence."[31] The Government initially has the burden of producing evidence to establish a potentially disqualifying condition under the Directive. Once the Government has produced substantial evidence of a disqualifying condition, under Directive ¶ E3.1.15, the Applicant has the burden of persuasion to present evidence in refutation, explanation, extenuation or mitigation, sufficient to overcome the doubts raised by the Government's case. The burden of disproving a mitigating condition never shifts to the Government.

---

[29] Applicant Exhibit C (Letter from Facility Security Officer, dated May 5, 2008).

[30] Applicant Exhibit B (Certificate signed by a Lieutenant General, USAF, and Letter from Program Manager, dated January 27, 2007).

[31] "Substantial evidence [is] such relevant evidence as a reasonable mind might accept as adequate to support a conclusion in light of all contrary evidence in the record." ISCR Case No. 04-11463 at 2 (App. Bd. Aug. 4, 2006) (citing Directive ¶ E3.1.32.1).

A person who seeks access to classified information enters into a fiduciary relationship with the Government predicated upon trust and confidence. This relationship 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 include, by necessity, consideration of the possible risk the 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.

Section 7 of Executive Order 10865 provides that 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." Accordingly, nothing in this Decision should be construed to suggest that I have based this decision, in whole or in part, on any express or implied determination as to Applicant's allegiance, loyalty, or patriotism.

Analysis

Guideline K, Handling Protected Information

The security concern relating to the guideline for Handling Protected Information is set out in AG ¶ 33:

> 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 willingness and ability to safeguard such information, and is a serious security concern.

The guideline notes several conditions that could raise security concerns. Under AG ¶ 34(g) "any failure to comply with rules for the protection of classified or other sensitive information" is potentially disqualifying. Department Counsel has identified this as the sole condition of this particular guideline possibly pertinent to this case,[32] and I concur. Applicant purportedly violated two rules. First, there was some otherwise unidentified and unspecified rule regarding permitting access to the facility when he drove onto the base, or as referred to by his then-Facility Security Officer, "snuck" her onto the base, during a time period in which he was to work and his companion had no legitimate business reason for being there. The actual "rule" has not been specified, detailed, discussed, or otherwise offered by the Government. It is impossible to determine if a spouse, companion, or driver who accompanies a cleared employee onto the base is also violating the supposed rule. According to the Government, at that time, her mere presence on the base required advanced permission for her to enter the base, regardless of her status. It should be noted, however, that this aspect of the argument is not alleged in the SOR, for the SOR allegation only refers to his "attempt" to bring the

[32] Tr. at 72.

unauthorized person into the classified area elsewhere referred to as the laboratory, but not the base itself.

The other aspect of the case refers to his purported "attempt" to bring his companion into the secured laboratory. The Government has presented an Adverse Information Report that Applicant had attempted to do just that, but was prevented from doing so by an unidentified employee. Applicant has countered that report with evidence in support of his contention that his companion needed to use the restroom so they drove to the unsecured building where he worked, entered it, and he escorted her to the restroom which was outside of the secured laboratory. He never took, or attempted to take, her into the laboratory itself. Except for the evidence submitted by Applicant, the record is silent regarding the location or security status of the restroom. I found Applicant's statement at the hearing to be consistent and credible. Because of the paucity of evidence contradicting him, I find that AG ¶ 34(g) is refuted by Applicant's more compelling and plausible evidence.

The guideline also includes examples of conditions that could mitigate security concerns arising from handling protected information. Under AG ¶ 35(a), the disqualifying condition may be mitigated where "so much time has elapsed since the behavior, or it has happened so infrequently or under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or good judgment." Similarly, AG ¶ 35(b), may apply where "the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities."

In this instance, I will assume the purported "security violations" occurred on March 23, 2005—three years before the date of the hearing—and Applicant was briefly put on administrative leave and, in part, because he had already submitted his notice intending to take another job with a competitor, terminated. Whether his punishment and termination were appropriate due to the circumstances, or due to rumor or innuendo, or simply retaliation and reprisal for attempting to join a competitor is unclear. What is clear is that since that time, after being closely *monitored* by his current Facility Security Officer for 18 months, Applicant was selected and *trained* to be COMSEC Custodian, a position he has handled with "superior results." Applicant has clearly maintained and demonstrated a "positive attitude toward the discharge of security responsibilities." Considering the totality of the evidence, I find that, assuming AG ¶ 34(g) is established, then AG ¶¶ 35(a) and 35(b) apply to mitigate the security concerns.

Guideline E, Personal Conduct

The security concern relating to the guideline for Personal Conduct is set out in AG ¶ 15:

> 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.

The following will normally result in an unfavorable clearance action or administrative termination of further processing for clearance eligibility:

> (a) refusal, or failure without reasonable cause, to undergo or cooperate with security processing, including but not limited to meeting with a security investigator for subject interview, completing security forms or releases, and cooperation with medical or psychological evaluation;
>
> (b) refusal to provide full, frank and truthful answers to lawful questions of investigators, security officials, or other official representatives in connection with a personnel security or trustworthiness determination.

The guideline notes several conditions that could raise security concerns. Under AG ¶ 16(b), "deliberately providing false or misleading information concerning relevant facts to an employer, investigator, security official, competent medical authority, or other official government representative" is potentially disqualifying. Similarly, under AG ¶ 16(c), "credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any other 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 properly safeguard protected information" may raise security concerns.

In addition, AG ¶ 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 that 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 government protected information:

(2) disruptive, violent, or other inappropriate behavior in the workplace;

(3) a pattern of dishonesty or rule violations;

(4) evidence of significant misuse of Government or other employer's time or resources," may apply.

Applicant has admitted he "falsified" his timecard pertaining to March 23-24, 2005, but explained that was the acceptable practice in place with his supervisor covering flexible time or overtime work. If such informal practice was acceptable to the supervisor is only one aspect of the issue, because it apparently was not acceptable to the employer. Unfortunately, the Adverse Information Report does not address this issue other than to say Applicant "falsified his timecard." As to the falsified timecard, I find AG ¶¶ 16(b), 16(c), and 16(d) apply in this case. As to the alleged "attempt to bring an unauthorized person into the secured laboratory, I find AG ¶ 16(c) applies.

The guideline also includes examples of conditions that could mitigate security concerns arising from personal conduct. Under AG ¶ 17(c), the disqualifying condition may be mitigated where "the offense is so minor, or so much time has passed, or the behavior is so infrequent, or it happened under such unique circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment." Similarly, AG ¶ 17(d) may apply where the evidence shows "the individual has acknowledged the behavior and obtained counseling to change the behavior or taken other positive steps to alleviate the stressors, circumstances, or factors that caused untrustworthy, unreliable, or other inappropriate behavior, and such behavior is unlikely to recur." Also, AG ¶ 17(f) may apply where "the information was unsubstantiated or from a source of questionable reliability."

Falsifying a timecard is not a minor offense. However, in this instance, Applicant contends the informal practice was acceptable to his supervisor, even if it may not have been acceptable to the employer. Nevertheless, three years have passed since the incident, and it was apparently an isolated action identified by his employer. Neither alleged action by Applicant constituted a pattern of dishonesty or rule violations. After being under intense scrutiny by his current employer for over 18 months, the circumstances have changed, the conduct has not recurred, and it is not likely to recur. As to the falsified timecard, I find AG ¶¶ 17(c) and 17(d) apply. As to the alleged "attempt to bring an unauthorized person into the secured laboratory, I find AG ¶¶ 17(c) and 17(f) apply.

Whole Person Concept

Under the whole person concept, the Administrative Judge must evaluate an Applicant's eligibility for a security clearance by considering the totality of the Applicant's conduct and all the circumstances. The Administrative Judge should consider the nine adjudicative process factors listed at AG ¶ 2(a):

> (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 extent to which participation is voluntary; (6) the presence or absence of rehabilitation and other permanent 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.

Under AG ¶ 2(c), the ultimate determination of whether to grant eligibility for a security clearance must be an overall common sense judgment based upon careful consideration of the guidelines and the whole person concept.[33]

I considered the potentially disqualifying and mitigating conditions in light of all the facts and circumstances surrounding this case. In March 2005, Applicant informed his PM of an offer of employment from a competitor, entered the military facility with a friend in his automobile, and accompanied her to the unsecured restroom near his secured laboratory. Although he was supposed to be working, he apparently had an informal flexible work schedule and entered what might be considered constructive information on his timecard. Nevertheless, the information was not accurate, and Applicant admitted the time card did not contain accurate information. Some form of inquiry or investigation was performed and Applicant was placed on administrative leave and terminated. As a result, because he was now barred from the facility, the offer of employment by the competitor was withdrawn. (*See* AG ¶¶ 2(a)(1), 2(a)(2), 2(a)(3), 2(a)(5), and 2(a)(7).

The two components of the isolated episode, the disputed issue of bringing an "unauthorized" person on base and purportedly "attempting" to bring her into a classified laboratory, as well as the falsification of the timecard, both occurred over three years before the hearing. Additionally, since that time, Applicant was closely *monitored* for 18 months, and eventually selected and *trained* to be COMSEC Custodian. He has handled the position with "superior results." And, he has clearly maintained and demonstrated a "positive attitude toward the discharge of security responsibilities." As such, there appears to be little likelihood of recurrence and the potential of pressure, coercion, exploitation, or duress because of the incident(s) is low.

Overall, the record evidence leaves me without questions or doubts as to Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude Applicant mitigated the security concerns arising from his handling protected information and personal conduct concerns.

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 K:	FOR APPLICANT
Subparagraph 1.a:	For Applicant
Subparagraph 1.b:	For Applicant
Subparagraph 1.c:	For Applicant

[33] Although I find Applicant's conduct mitigated under the individual guidelines as previously indicated, I also separately find security concerns mitigated under the whole person concept.

Paragraph 2, Guideline E:	FOR APPLICANT
Subparagraph 2.a:	For Applicant
Subparagraph 2.b:	For Applicant

Conclusion

In light of all of the circumstances presented by the record in this case, it is clearly consistent with national security to grant Applicant eligibility for a security clearance. Eligibility for access to classified information is granted.

_____
ROBERT ROBINSON GALES
Chief Administrative Judge