DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
----------	)	ISCR Case No. 07-15843
SSN: ----------	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Emilio Jaksetic, Esq., Department Counsel
For Applicant: Leslie McAdoo-Gordon, Esq.

December 18, 2008

_____

Decision

_____

ABLARD, Charles D., Administrative Judge:

Applicant mitigated the security concerns raised by his handling protected information and alleged under Guideline E (Personal Conduct), and Guideline K (Handling Protected Information). Eligibility for access to classified information is granted.

On December 21, 2007, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) to Applicant, detailing the security concerns under Guideline E, Personal Conduct, and Guideline K Handling Protected Information. The action was taken under Executive Order 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the revised adjudicative guidelines (AG) promulgated by the President on December 29, 2005, and effective within the Department of Defense for SORs issued after September 1, 2006.

Applicant answered the SOR in writing on January 22, 2007, and requested a hearing before an Administrative Judge. The case was assigned to me on June 10,

2008. DOHA issued a notice of hearing on June 20, 2008, for a hearing on August 12, 2008. I convened the hearing as scheduled. The Government offered Exhibits 1 through 32, which were received without objection. The exhibits include many government and corporate documents relating to requirements imposed by the National Industrial Security Program Operating Manual (NISPOM) (Exhs. 4 and 5), and the implementation of those documents by the corporate employer.

Applicant testified on his own behalf, and submitted Exhibits A-L which were admitted without objection. An index for both sets of documents was submitted and appended to each one. DOHA received the transcript of the hearing (Tr.) on August 20, 2008.

Findings of Fact

Applicant is a 46-year-old test supervisor for a defense contractor with 11 technicians working for him at 15 test stations that are considered classified because of the test data that is inputted on them. He attended a community college and has an associate's degree. He served in the Navy for 21 years and was discharged in 2001 as an E-7. He has held a security clearance during and since his military service for a total of 28 years (Exh. F). He has worked for his present employer and the former owner since his discharge from the Navy. The allegations center around a series of security incidents involving his staff of technicians and three in which he solely was a participant.

Sometime in early 2003, Applicant was given the additional duty of Information Systems Security Officer (ISSO) for his group. Applicant was briefed on his duties by the ISSM when he was named ISSO and given some additional training. The total training given to Applicant is detailed at Exh. 32 (a-p). His staff of technicians was also given annual training. After several of the staff violations occurred, Applicant requested the ISSM to provide training every six months. His request was granted (Tr. 103).

At the time the additional duties were assigned, Applicant was working ten hours a day and weekends on a rush project for a customer of his employer (Tr. 25 and 186). During the next three years or until July 2006 a number of security incidents occurred which are the subject of five of the allegations in the SOR. These incidents were committed by one or more of the eleven members of the technical staff whom he supervised. Applicant and the violators were both held responsible. Applicant was counseled, given written warnings, and, for the last incident, suspended for three days without pay. All of these incidents are SOR allegations (SOR ¶¶ 1 (a., b., d., e., and g.)). Two other violations occurred (SOR ¶¶ 1 (c. and f.)) for which he was personally involved and admits in his answer.

The security incidents by Applicant's staff were as follows:

1. Unauthorized use of another employee's password in June 2004 (SOR ¶ 1 (a)) (Exh. 7);

2. Improper installation of software in June 2004 (SOR ¶ 1 (b));

3. Improper access to test station in May 2006 (SOR ¶ 1 (e.)) (Exh. 26);

4. A trusted down-loading incident (taking unclassified information from a classified work station) on March 3, 2006, (SOR ¶ 1 (d)) (Exh. 25); and,

5. A second incident involving trusted downloading by an employee who had not been trained to do so occurred on July 27, 2006 (SOR ¶ 1 (g)) (Exh. 28).

Applicant observed the May 2006 violation and reported it to his superiors. Both Applicant and the staff member were reprimanded (Tr.45-47). Applicant also advised the employee in the July 2006 incident that he was not qualified to do downloading and suggested others who should do it for him. However, the employee ignored his Applicant's instruction and did it himself (Tr. 49). After the second trusted downloading incident by his staff members in 2006, Applicant's ISSO duties were terminated later in the year (Exh. 28).

According to the Master System Security Plan adopted by Applicant's company (Exh. 11), the Information System Security Manager (ISSM) "has the oversight responsibility for the development, implementation, and evaluation of the facility's IS Security Program." The ISSM appoints and delegates certain responsibilities to an ISSO (Exhs. 10 and 11). The company had a classified test station which consisted of a series of classified computers in a secured area. Everyone who worked in the area had a clearance. It was the responsibility of the ISSM to set up the initial user accounts and access privileges.

The first alleged security violation for which Applicant admits responsibility (SOR ¶1 (c)) was in October 29, 2005, when he failed to properly set an alarm in a protected area as he left the building (Exh. 24). The alarm should have buzzed when operational but it did not. He left the building before making certain that it was properly set. He was given a written warning. The alarm system had created problems for others as well as for him according to his supervisor (Exh. B). The protected area of the building was locked and no compromise of security or tampering was discovered (Exh. 24 p. 2).

The second alleged security violation for which Applicant admits responsibility (SOR ¶1 (f)) occurred on June 26, 2006, (Exh. 27) when he was called by one of his staff on an unsecure phone while he was on the way to the airport at the beginning of a weekend. The employee needed access to a classified safe. Applicant gave him the combination over the phone but advised him to have the combination immediately changed. However, the staff member did not follow his instruction and waited until the following Monday morning to have the combination changed. The incident was recorded in Applicant's personnel file for 18 months, and he and his staff member were required to re-take safe responsibility training. He was also given a written warning for incident.

The last alleged incident in which Applicant was personally involved was on March 19, 2007, eight months after his ISSO duties were terminated (SOR ¶1 (i)) (Exh. 29). A security audit by a Defense Security Service representative found six unmarked

media disks on Applicant's desk and, according to the SOR, approximately 75 unmarked media disks on a shelf behind his desk. Applicant believed there were only a total of 50. The security incident report on this matter indicated confusion as to the extent of markings on the disks and the location of the disks at issue (Exh. 3, p. 6).

All the disks had been in the possession of a former employee who recently died. Applicant was asked by his manager to review the disks, all of them unmarked, and determine whether classified material was on them. This was an extra duty which he had been doing over a three month period as of July 2007. He had reviewed the disks on the shelf which were in a box marked "unclassified" and determined that there was no classified information on any of them, but had not affixed individual markings on the disks. He had not reviewed the six disks on his desk and they were unmarked. For this incident he was suspended without pay for five days and removed from supervisory responsibility for classified information (Tr. 82-100).

Counsel for Applicant contended at the hearing that the failure to apply markings was not a violation of corporate regulations or of Section 4-212 of the NISPOM (Exh. 4). That section provides that wholly unclassified material need not be marked unless two conditions apply. There was no evidence submitted at the hearing to show that those conditions were applicable. A contra corporate position of the ISSM appears in the record that indicates all disks must be individually marked whether classified or unclassified (Exh. 29).

An Administrative Inquiry was conducted in 2006 by the Defense Security Service concerning the incidents that had occurred as of that time. A report was issued on August 23, 2006 (Exh. 2) finding a pattern of negligence and forwarding the matter to DISCO for appropriate action. An administrative inquiry (ASC) was conducted by the corporate employer after the discovery of the last incident in March 2007. At that time no punishment for the 2007 incident had been imposed. A report was issued on March 28, 2007 (Exh. 31). It stated that Applicant "was involved in four minor security incidents (deviations), one infraction and one violation (involving compromise of classified materials) in the past 18 months." The recommendations of the ASC were based on the one violation (communicating safe combination over phone), the infraction (alarm issue), and the most recent incident (disk marking) which it characterized as a "deviation". The deviations involving staff members were discounted as indicative of security leadership weakness.

The inquiry concluded that Applicant was unable or unwilling to comply with security rules and there was a clear pattern of negligence. The inquiry recommended a written warning, an adverse information report to DSS, and counseling of Applicant and his manager on importance of compliance. In addition the report recommended that the manager with access to the closed area should brief all employees on the importance of marking all media. The report recommended no follow up activity or any changes in policy or procedure. The report relied on the Progressive Discipline for Security Incidents guidelines (Exhs. 19 and 20).

One allegation, (SOR ¶1 (h)), does not allege any specific conduct but recites the facts alleged noting that two incidents by Applicant's staff were repeat offenses and five of them involved classified computers. It recites the DSS conclusion that the facts indicate a pattern of "negligence and carelessness" and that an Administrative Inquiry (ASC) was conducted and forwarded to DISCO. These facts are consistent with the record.

Applicant had no security violations in his career before he was named ISSO. At the time of the termination of his additional duty as ISSO, a new full time ISSO was named. After he was terminated as an ISSO in 2006, he had one security incident that involved him personally (SOR ¶ 1 (i)) concerning unmarked media disks on March 19, 2007. He has had no security incidents since the 2007 incident (Exhs. F and I).

Three letters from Applicant's supervisors at three supervisory levels, and numerous performance appraisals, evaluations, and awards were submitted in evidence (Exhs. A, B, and C). These letters describe him as scrupulous and conscientious about security issues. They all recommended that he retain his security clearance. The evaluations describe Applicant as a dedicated, conscientious, and highly-valued employee. He is described as hard working, ethical, honest, trustworthy, and reliable. Applicant is divorced and has three adult children (Tr. 21-24).

Policies

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

These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, administrative judges apply the guidelines 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 decision.

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.

Under Directive ¶ E3.1.14, the Government must present evidence to establish controverted facts alleged in the SOR. Under Directive ¶ E3.1.15, the applicant is

responsible for presenting "witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by the applicant or proven by Department Counsel." The applicant has the ultimate burden of persuasion as to obtaining a favorable security decision.

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. The Government reposes a high degree of trust and confidence in 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 adverse 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." *See also* EO 12968, Section 3.1(b) (listing multiple prerequisites for access to classified or sensitive information).

Analysis

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.

AG ¶ 16 describes several conditions that could raise a security concern and may be disqualifying. The following is the only one that is potentially applicable:

> (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.

Applicant's conduct was also alleged under Guideline K (Handling Protected Information), as addressed below. That conduct constitutes credible adverse information in another adjudicative issue area that may not be 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, and unwillingness to comply with rules and regulations. It is also personal conduct that could create a vulnerability to exploitation, manipulation, or duress.

AG ¶¶ 16(c) is sufficiently raised for consideration. Conditions that could mitigate Personal Conduct security concerns are provided under AG ¶ 17. The following are potentially applicable:

> (c) 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;
>
> (d) 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; and
>
> (e) the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress.

The discussion under the guideline for Handling Protected Information is equally appropriate for this guideline. Additionally, Applicant has been open and honest about the violations in his testimony and earlier statements. This has reduced any potential vulnerability to exploitation, manipulation, and duress. The above mitigating conditions are applicable.

Guideline K, Handling Protected Information

The same allegations alleged under Guideline E as security concerns were also alleged under Guideline K Handling Protected Information 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.

AG ¶ 34 describes conditions that could raise a security concern and may be disqualifying. The following are potentially applicable:

> (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;

(c) loading, drafting, editing, modifying, storing, transmitting, or otherwise handling classified reports, data, or other information on any unapproved equipment including but not limited to any typewriter, word processor, or computer hardware, software, drive, system, gameboard, handheld, "palm" or pocket device or other adjunct equipment;

(g) any failure to comply with rules for the protection of classified or other sensitive information; and

(h) negligence or lax security habits that persist despite counseling by management.

AG ¶ 33 addresses "[d]eliberate or negligent failure to comply with rules and regulations for protecting classified or other sensitive information." Applicant's actions regarding the violations for which he was personally involved were not deliberate security violations. Negligence is commonly defined as the failure to use reasonable care under the circumstances. It is the doing of something which a reasonably prudent person would not do, or the failure to do something which a reasonably prudent person would do under like circumstances. The government characterized Applicant's actions as careless or negligent to which Applicant admitted. After considering all the evidence, I conclude that he was negligent in those three incidents. Applicant's actions were sufficient to raise security concerns under AG ¶¶ 34(g) and (h) for consideration.

Conditions that could mitigate Handling Protected Information security concerns are provided under AG ¶ 35. The following are potentially applicable:

(a) 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; and

(b) the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities.

Applicant was chosen to be an ISSO in addition to his regular duties. He had never held the duty before but he trained for it and attempted to insure through accelerated training that his staff was prepared. However, incidents occurred caused by others for which he was held responsible and given punishment despite his best efforts to insure that they were not repeated. He has been appropriately disciplined for all of the incidents including the ones actually committed by his staff without his knowledge, direction, or permission.

Applicant no longer has the ISSO additional duties. He approaches the discharge of his security responsibilities with a positive attitude and has had no further difficulties since the disk marking incident. While he had three violations in which he was personally involved as the administrative inquiry found, he was punished for all of them. The first two resulted in warnings and he was suspended for five days without pay for the third. However, the three incidents in which Applicant was personally involved were quite different as to the type of security issues involved and the classification of the three as an infraction, a violation, and a deviation.

The Progressive Discipline process applies increasing penalties as sequential violations of a similar nature occur. Several of those for which his staff was involved were similar in that they involved the use of classified equipment. The discipline did increase for the last of the two trusted downloading staff incidents that occurred within a three month period. The second one resulted in removal of ISSO responsibilities from Applicant. No further action was recommended by the ASC corporate inquiry.

While the conclusion of the ASC is not binding on the government which characterized them at the hearing as only "opinions" that neither bound the government, nor precluded further government action, the ASC makes rational and sensible findings in view of the circumstances of this case. I find that Applicant has mitigated the security concerns.

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.

I considered the potentially disqualifying and mitigating conditions in light of all the facts and circumstances surrounding this case. Security violations are one of the strongest possible reasons for denying or revoking access to classified information, as they raise very serious questions about an applicant's suitability for access to classified information. Once it is established that an applicant has committed a security violation,

he or she has a very heavy burden of demonstrating that he or she should be entrusted with classified information. Because security violations strike at the very heart of the industrial security program, an administrative judge must give any claims of reform and rehabilitation strict scrutiny.

In many security clearance cases, applicants are denied a clearance for having an indicator of a risk that they might commit a security violation (e.g., alcohol abuse, delinquent debts or drug use). No such indicator or any other indicator has occurred in this case.

The DOHA Appeal Board has held that supervisors can be held responsible for security violations by members of their staff. The most recent decision so holding was ISCR Case No. 06-21537 (App. Bd. February 2, 2008) where the Board reversed a decision granting clearance to a supervisor who had a pattern of gross negligence, and had failed to favorably respond to the security violations or to have a positive attitude towards security duties. The facts of this case do not indicate that either failure is applicable to Applicant.

Security violation cases reveal more than simply an indicator of risk but in ISCR Case No. 03-26888 (App. Bd. Oct. 5, 2006) cited by the government, the applicant was found to have disregarded procedures and tried to conceal violations. No evidence of such conduct was established in this matter and, in fact, Applicant reported at least one incident when he was the only person to know of it, and he was punished with the staff violator. He also directed another staff member not to do what he then proceeded to do that resulted in a security incident. The frequency and duration of the security violations are also aggravating factors, but in ISCR Case no 97-0435 (App. Bd. July 14, 1998) the case cited by the government for this issue, there was evidence of deliberate security violations over a ten year period.

The three incidents for which Applicant was personally involved were viewed by the ASC as a single violation, a single infraction, and a single deviation. They were each a different type of security violations committed over a period of 18 months with little, if any, consistent pattern as to the facts or even the gravity of the incidents.

Applicant is a dedicated, trustworthy employee who was in over his head as an ISSO. His duties were more than he could effectively perform in addition to his basic required duties. He could not watch every action of his staff and others in the work environment. Yet he was held responsible for them. He took steps to insure that adequate training was provided to insure that violations did not occur. He did as much as could be expected of him. There is no real potential for pressure, coercion, exploitation, or duress and the likelihood of continuation or recurrence of the same behavior is very low. He has met his heavy burden.

Applicant's conduct at the hearing and the quality of the answers to questions from both of the counsel and from me indicated complete honesty, and a willingness to accept responsibility for those actions for which he should have accepted responsibility. He did not attempt to shift blame to others but realistically explained the difficulty of

attempting to insure full compliance by all members of the staff and others who had access to the classified stations. The government conceded at the hearing that the case was "somewhat circumstantial" (Tr. 159) and clearly it is. I am convinced that there are no lingering concerns about his judgment, reliability, and trustworthiness that justify removal of his security clearance.

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

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: FOR APPLICANT

Subparagraphs 1.a-1.I: For Applicant

Paragraph 2, Guideline K: FOR APPLICANT

Subparagraph 1.a: For Applicant

Conclusion

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

_____
Charles D. Ablard
Administrative Judge