DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 07-06786
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Ray T. Blank, Jr., Esq., Department Counsel
For Applicant: David P. Price, Esq.

May 22, 2008

Decision

LOUGHRAN, Edward W., Administrative Judge:

Applicant mitigated the security concerns raised by his handling protected information and personal conduct. Eligibility for access to classified information is granted.

On October 9, 2007, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) to Applicant, detailing the security concerns under Guideline K, Handling Protected Information and Guideline E, Personal Conduct. 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 October 25, 2007, and requested a hearing before an Administrative Judge The case was assigned to me on January 17, 2008. DOHA issued a notice of hearing on March 14, 2008. I convened the hearing as

scheduled on April 10, 2008. The Government offered Exhibits (GE) 1 through 8, which were received without objection. Applicant testified on his own behalf, called five witnesses, and submitted Exhibits (AE) A-1 through A-20 and B-1 through B-29, which were received without objection. DOHA received the transcript of the hearing (Tr.) on April 22, 2008.

Procedural and Evidentiary Rulings

Request for Administrative Notice

The SOR references paragraphs of the National Industrial Security Program Operating Manual (NISPOM) (5220.22-M), dated January 1995, and also the NISPOM dated February 28, 2006. Department Counsel orally requested that I take administrative notice of the referenced sections of both versions of the NISPOM. Department Counsel did not offer a copy of the requested provisions. The Federal Rules of Evidence serve as a guide at DOHA hearings.[1] The Appeal Board has noted that administrative or official notice in administrative proceedings is broader than judicial notice under the Federal Rules of Evidence and is appropriate for DOHA hearings.[2] Rule 201 of the Federal Rules of Evidence addresses judicial notice:

> **(d) When mandatory.** A court shall take judicial notice if requested by a party and supplied with the necessary information.
>
> **(e) Opportunity to be heard.** A party is entitled upon timely request to an opportunity to be heard as to the propriety of taking judicial notice and the tenor of the matter noticed. In the absence of prior notification, the request may be made after judicial notice has been taken.

I withheld ruling on the request and directed Department Counsel to submit a copy of the requested sections to myself and Applicant's counsel by April 25, 2008, with Applicant's counsel to file any objections by May 2, 2008. Department Counsel did not submit any matter by the assigned date. Department Counsel verified after the assigned date was past that he did not submit the documentation. He did not request additional time to submit any matter. Based upon the Government's failure to provide the necessary information and the inability of Applicant to be heard on the matter, the request for administrative notice is denied.

GE 6 (Master System Security Plan)

GE 6 is the Master System Security Plan at Applicant's company. It is dated September 2001 and revised March 2005. The conduct alleged in SOR ¶¶ 1.a and 1.b occurred before the revision of the Plan. The Plan contains a description of the changes to the plan, which included "[i]dentified security personnel" and "[e]laborated on the

[1] Directive ¶ E3.1.19.

[2] ISCR Case No. 03-21434 at 3 (App. Bd. Feb. 20, 2007).

roles of personnel." I held the record open until April 25, 2008, to allow the Government to submit a copy of the original Plan that was in effect during the first two SOR allegations. Applicant's counsel had until May 2, 2008, to file any objections and rebuttal material. No additional evidence was submitted.

Findings of Fact

Applicant is a 45-year-old senior engineering specialist for a defense contractor. He attended a few years of college and has a diploma from a technical school awarded in 1985. He started working for a defense contactor in 1985, and has held a security clearance since then. He has worked for his same management team since 1985, but the companies have changed hands and went through name changes. He is married and has two children, ages 16 and 10.[3]

In about March 2004, an employee at Applicant's company, in an unclassified area, scanned a large amount of documents into an electronic file. He did not believe the documents contained any classified information. He e-mailed the file in an attachment to Applicant. Applicant forwarded the e-mail to several people without reading the attachment. He then started reading the attachment and realized it contained information that could be classified. He immediately called his supervisor and the company's security officer and reported it. He called all the recipients and told them not to open the attachment. He was able to recall the e-mail without the information being compromised.[4] Applicant was issued a written Security Violation Notice by Interdepartmental Correspondence on March 5, 2004. It stated:

> Though unintentional, your actions are in direct violation of established security procedures to properly protect classified information. As a result this Security Violation Notice is being issued to you. You are reminded that the handling and protection of classified information requires extreme caution and attention to individual responsibility in order to preclude compromise or loss of classified information, customer criticism, and possible impact on our company's clearance by the Government. Subsequent violations may result in further disciplinary actions to include termination.[5]

According to the Master System Security Plan at Applicant's company, 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 Information System Security Officer (ISSO).[6] The company had a classified test station which consisted of a series of

[3] Tr. at 88, 148-149, 200-201; GE 1.

[4] Tr. at 47-51, 149-155; Applicant's Answer to the SOR; GE 3; AE A-1.

[5] GE 3.

[6] GE 6.

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 optimum way of accomplishing this for the company's project would be to create a common user "desktop" with all the access privileges and permissions set up. Each user would then be given their own copy of this desktop with their own unique login. For technical reasons, they were unable to do this and a common desktop was unattainable. Instead each user's desktop was set up uniquely, often with different privileges. Technicians received a limited set of privileges to run certain software and access data files. Test engineers had somewhat more privileges such as accessing the test software. The ISSO had limited administrator privileges to create the user accounts and review the computer security logs. The ISSM had full administrator rights to install/remove software and all the lesser privileges of the others.[7]

Applicant was orally named an ISSO some time in or before September 2004. The standard briefing was an overview provided by the ISSM on an as-needed basis to explain the basic rules. Applicant's briefing on his duties by the ISSM took about five minutes. Additional training was minimal or nonexistent.[8] The test engineer who designed the test station in question described the ISSO:

> A person is assigned to be the Security Custodian for the station. He is responsible for creating and disabling the user accounts as necessary, and to perform periodic audits of the security logs. This person is referred to as the ISSO (Information System Security Officer). He is typically not a computer security expert and receives only the most rudimentary training to perform his duties. I should note that the ISSO receives no additional compensation or privileges for doing this duty. In reality the most likely outcome of being an ISSO is that at some point you will receive a security violation, often for something that occurs on a station over which you had little or no control. Such is the case with [Applicant].[9]

A security review on September 14, 2004, revealed potential security violations. Applicant was formally designated the ISSO in writing with his delegated duties enumerated on September 23, 2004. Part of his listed duties included performing IS weekly audit reviews. He signed his Authorization and Briefing Form on the same day.[10]

Applicant was issued a Security Violation Notice (Written Warning) by Interdepartmental Correspondence on September 24, 2004. It stated:

> On September 14, 2004 it was found that an unapproved computer had been connected to a system for at least three weeks in which you were

[7] Tr. at 53-90; AE A-5.

[8] Tr. at 86, 167-168; AE A-5.

[9] AE A-5.

[10] Tr. at 167, 173; GE 4, 7, 8.

> the Information System Security Officer. A check of system logs indicate that the required weekly audit reviews had not occurred since the system was established. Furthermore, you had admitted to allowing system access beyond what had been established for user levels.
>
> Your failure to perform required ISSO duties are in direct violation of established security procedures to properly protect classified information. As a result this Security Violation Notice is being issued to you. Furthermore, this is your second security violation (unrelated) within the past twelve months. This notice serves as a written warning reminding you that the handling and protection of classified information requires extreme caution and attention to individual responsibility in order to preclude compromise or loss of classified information, customer criticism, and possible impact on our company's clearance by the Government. A similar subsequent violation will result in an adverse information report being submitted to the Government and may result in further disciplinary actions to include termination.[11]

The security violation referencing the unapproved computer resulted from one of the test engineers who had an unapproved computer that was linked to the classified system. Applicant had also not completed the required weekly audit reviews. The test engineer who designed the test station at issue wrote a statement and testified on Applicant's behalf. He has also served as an ISSO. He stated that "the security logs are, at best, very cryptic and it is only recently (a few months ago) that our local DSS representative has even explained what kind of log entries to look for as signs of security problems." Additionally, some of the computers were running programs constantly for testing for as long as a few weeks. Automated testing took between 14 to 18 hours to run. If the user logged off the system while it was running, the system would shut down and have to be restarted and rebooted, which would require the program to start from the beginning. An audit would require the user to log off the system. The final aspect of the security violation is that Applicant permitted the practice of people working while logged onto the system with other people's log-in, including Applicant's. This was a common practice and was necessary to run the tests. Passwords were not shared; it was done with everyone's knowledge; and all the workers had clearances. There is nothing specifically in the company's Master System Security Plan that prohibits this practice and it was eventually approved.[12]

The project engineer testified and admitted that Applicant should have been removed as ISSO after the second Security Violation Notice for his own protection. What was stressed after the second Security Violation Notice was that Applicant review the computer security logs and complete the weekly audit reviews. There is no evidence that this ever became a concern again. Running programs while logged onto the system with other people's log-in was not emphasized as a concern. The project engineer

[11] GE 3.

[12] Tr. at 65-67, 79-85, 119-120, 159-160, 167-169; AE A-5.

testified that he did not realize it was against the rules to do so until after Applicant's third Security Violation Notice.[13] The test engineer who designed the test station also testified. I asked him:

> Q: The rules regarding logging on and off that gave a lot of problems, were they established by the company, by the NISPOM, by DSS, or a combination, or do you know?
>
> A: Honestly I don't know exactly.[14]

Applicant was issued a Security Violation Notice (Final Written Warning) by Interdepartmental Correspondence on October 30, 2006, stating:

> On October 26th, 2006, you had admitted that you were logged into your administrator account on an unapproved classified computer for the purpose of conducting a classified test which is unauthorized for that purpose. Furthermore, the account had remained logged in for fourteen days and you had subsequently used the open account to conduct additional tests suggesting that you were aware others were using your administrator account.
>
> Using your ISSO account to perform classified testing is in direct violation of established security procedures. . . A similar subsequent violation will result in termination of your employment.[15]

The guidelines as far as users operating the system while logged onto another's account were unclear. The problem with Applicant permitting others to be logged onto the system with his log-in is that they could potentially access security logs that only the ISSO should have access to. Applicant did not become aware that he had additional access as an ISSO until the hearing. At some point after Applicant received his third Security Violation Notice, the implementation of the guidelines changed to essentially permit the system to stay logged onto the same user until the program ran its course. ISSOs were still prohibited from permitting others to access the system with their ISSO account. Applicant was removed as an ISSO after the third violation. No classified information was compromised as a result of the alleged security violations.[16]

Five witnesses testified on applicant's behalf. Twenty letters and numerous performance appraisals, evaluations, awards, and accolades were submitted in evidence. Applicant is a conscientious, dedicated, and highly-valued employee. He is

[13] Tr. at 124-128, 133-134.

[14] Tr. at 88.

[15] GE 5.

[16] Tr. at 59-60, 118-120, 131-134, 177-179, 195.

described as hard working, ethical, honest, trustworthy, and reliable. He is recommended to retain his security clearance.

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 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.

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;
>
> (b) collecting or storing classified or other protected information at home or in any other unauthorized location;
>
> (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.

Applicant forwarded an e-mail without reading the attachment. When he read the attachment shortly thereafter, he realized that it contained classified information and took immediate remedial action, which included reporting it to his supervisor and security officer. This action satisfies the requirements of AG ¶ 34(c). However, AG ¶ 33 addresses "[d]eliberate or negligent failure to comply with rules and regulations for protecting classified or other sensitive information." Applicant's action was not deliberate. 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. After considering all the evidence, I conclude that the forwarding of the e-mail did not constitute negligent conduct.

Applicant's actions as listed in the second and third Security Violation Notices are sufficient to raise AG ¶¶ 34(g) and 34(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;
>
> (b) the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities; and
>
> (c) the security violations were due to improper or inadequate training.

Applicant was chosen to be an ISSO without any real training on his responsibilities. He was not formally designated the ISSO in writing with his delegated duties enumerated until September 23, 2004, the day before he was issued the second Security Violation Notice, but after the actions that formed the basis of the Notice. He still did not receive sufficient training to do his job. It was stressed that Applicant review the computer security logs and complete the weekly audit reviews. This behavior was not repeated. The practice of people running programs while logged onto other person's accounts continued. It is still unclear where the prohibition of this practice came from, as it is not in the company's Master System Security Plan, the witnesses could not identify who or what prohibited the practice, and the practice was eventually approved. ISSOs could not and are still prohibited from permitting others to log-in through their account as it allows access to security files that should be available only to the ISSO, ISSM, and the security officer. Because of the lack of proper training, he was unaware that he could access files as the ISSO that others could not. Applicant did not have a lax attitude toward security. He always approached his job with a view toward protecting classified information. He simply was ill-prepared for his additional security duties. He no longer has those additional duties. He approaches the discharge of his security responsibilities with a renewed vigor and a positive attitude. I find all three mitigating conditions to be applicable.

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 conditions that could raise a security concern and may be disqualifying. The following are 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; and
>
> (e) personal conduct, or concealment of information about one's conduct, that creates a vulnerability to exploitation, manipulation, or duress, such as (1) engaging in activities which, if known, may affect the person's personal, professional, or community standing.

Applicant's personal conduct was also alleged under the Handling Protected Information guideline, as addressed above. It 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(a) and 16(e) have been 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 conduct which has reduced any potential vulnerability to exploitation, manipulation, and duress. The above mitigating conditions are applicable.

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). Security violation cases reveal more than simply an indicator of risk.[17] The frequency and duration of the security violations are also aggravating factors.[18] Applicant is a hard working, dedicated, honest man who was in over his head as an ISSO. His problems were compounded by the almost complete lack of training. He focused on the big picture of safeguarding the classified information, but the devil is in the details, and he was not armed to handle the details. There is no real potential for pressure, coercion, exploitation, or duress and the

[17] ISCR Case No. 03-26888 (App. Bd. Oct. 5, 2006).

[18] ISCR Case No. 97-0435 at 5 (App. Bd. July 14, 1998).

likelihood of continuation or recurrence of the same behavior is very low. Applicant has met his heavy burden. I am convinced that there are no lingering concerns about his judgment, reliability, and trustworthiness.

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 K:	FOR APPLICANT
Subparagraphs 1.a-1.c:	For Applicant
Paragraph 2, Guideline E:	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.

_____
Edward W. Loughran
Administrative Judge