DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
----------	)	ISCR Case No. 08-02019
SSN: ----------	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government:
Jeff A. Nagel, Esquire, Department Counsel

For Applicant:
Kenneth M. Roberts, Esquire

November 10, 2009

DECISION

ROSS, Wilford H., Administrative Judge:

The Applicant submitted his Electronic Questionnaire for Investigations Processing on May 23, 2006 (Government Exhibit 1). On October 14, 2008, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) to the Applicant detailing the security concerns under Guidelines K (handling protected information), E (personal conduct), and M (misuse of information technology). 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 submitted an Answer to the SOR on November 5, 2008, and requested a hearing before an Administrative Judge. I received the case assignment on December 12, 2008. DOHA issued an original notice of hearing on December 16, 2008, and hearings were held on March 27, 2009, and October 2, 2009. The Government offered Government Exhibits 1 through 10, which were received without objection. Applicant testified on his own behalf, called three additional witnesses, and submitted Applicant's Exhibits A through V, and X, without objection. The post-hearing brief of the Applicant was marked Applicant's Exhibits W for identification only. DOHA received the final transcript of the hearing on October 13, 2009. The record closed on that date. Based upon a review of the case file, pleadings, exhibits, and testimony, eligibility for access to classified information is denied.

Findings of Fact

The Applicant is 55, married, and has a master's degree. He is employed by a defense contractor and seeks to obtain a security clearance in connection with his employment. The Applicant has worked for his current employer since 2006. All of the incidents alleged in the SOR occurred during his employment with another defense contractor [Company]. He was employed by the Company for 27 years, until December 2005.

Paragraph 1 (Guideline K - Handling Protected Information)

The Government alleges in this paragraph that the Applicant is not eligible for a security clearance because he has committed security violations.

Subparagraph 1.a. The Applicant's first security violation occurred on November 3, 2003. This violation was for misplacing the key to a classified storage area and departing the area before resolution of the incident. The key was found in the Applicant's office. The Applicant had to leave the area in order to pick up his six-year old son at a bus stop. (Government Exhibit 5, Exhibit 7 at 4; Transcript II at 11-14, 58-60.)[1]

Subparagraph 1.b. The Applicant's second security violation occurred in June 2004. The Applicant had a camera pass, which allowed him to take photographs at a Company facility. Areas in this facility contained classified material. On this occasion, he took a photograph of a part of a device, which he believed to be unclassified. However, he also knew that documentation showed the part to be classified, even though it was not. The facility security officer stated that the Applicant was advised "when in doubt do not take the picture." The part the Applicant took the picture of was later determined to be unclassified. (Government Exhibit 7 at 4, Exhibit 9; Transcript I at 101-104, 181-185; Transcript II at 14-19, 60-62; 100-107.)

[1]The transcript of the March 27, 2009, hearing will be identified as "Transcript I at xx." The transcript of the October 2, 2009, hearing will be identified as "Transcript II at xx."

Subparagraph 1.c. The Applicant's third security violation occurred in March 2005. This violation also involved the Applicant taking a photograph of a different part of the same device. Once again the Applicant thought, but did not know, that the part was unclassified. As before, this part was also shown in documentation to be classified. The incident report submitted by the facility security officer states that the Applicant was told "if he had any doubts an item was classified he was to have it authorized by a classifier before taking the picture." The part was subsequently determined to be unclassified. (Government Exhibit 4 at 1, Exhibit 7 at 4; Transcript I at 185-188; Transcript II at 18-22, 62-65, 107-109.)

The Applicant's Team Lead at the time of the events set forth under 1.b. and 1.c., above, testified that he was "shocked" and "aghast" that these events resulted in security violations being lodged against the Applicant. The witness explained in detail why he felt that these were not true violations and that the facility security officer did not understand how the camera pass system worked. (Transcript I at 182-185.)[2]

Paragraph 2 (Guideline E - Personal Conduct)

The Government alleges in this paragraph that the Applicant is ineligible for clearance because he has engaged in conduct which shows questionable judgment, lack of candor, dishonesty, or an unwillingness to comply with rules and regulations.

2.a. The Applicant's conduct, as set forth under Paragraph 1, above, will also be examined under Guideline E.

2.b. The Applicant admits that he installed personally-owned software on his company supplied computer sometime in 2005. He further stated that the software was Adobe Acrobat, and he removed it after being informed by the company IT (Information Technology) manager that unapproved software was not allowed on his computer. (Government Exhibit 3 at 1, and Exhibit 10; Transcript I at 111-112, 188-191; Transcript II at 22-28, 65-71.)

The Applicant did not admit at any time that he had installed other personally-owned software on his company computer. Specifically, software that would allow him to remove personal emails from his account and therefore "scrub" it. However, as further described under subparagraph 2.f., below, he did admit to deleting emails from his account, but through another method. In addition, no evidence was submitted by either side identifying any computer software program that would act in this fashion. Based on the state of the record, I find that this allegation is not proven as alleged. Accordingly, subparagraph 2.b. is found for the Applicant.

2.c., 2.d., 2.e., and 2.f. These four subparagraphs refer to a course of events, involving the Applicant's termination from the Company, and the aftermath. In order to provide continuity, they will be discussed together.

---

[2] *See also* Transcript I at 235-238, 257-260.

The Applicant was in charge of a building for the Company. Classified hardware was worked on in this building. On June 2, 2005, a piece of classified hardware came into the building. A particular part of this hardware contained an explosive charge. The building could only work on inert components. In other words, while explosive material could be in the building, it could not be worked on. The normal course of events for this piece of hardware was to return it to the vendor, which was not the Company, when work had to be done on the part containing the explosive charge. (Transcript I at 112-116, 151-152, 192-193, 201-202, 260-264.)

The Applicant gave instructions regarding the handling of the part containing the explosive charge that were, evidently, incorrect. In fact, the Applicant admitted at the hearing that his instructions had been "a mistake." (Transcript at 112.) These instructions were recorded in a computer generated report (Report). (Applicant's Exhibit Y.) Written copies of this Report, including the Applicant's instructions, were printed up for the file. The Applicant then left for the evening after giving his instructions. Later that day, the Applicant's instructions were superseded by his Team Lead and the situation was reported as a possible ordnance incident. It was emphasized by the Applicant, and two witnesses who worked with him at the Company at the time, that an unsafe situation never developed. (Government Exhibit 7 at 1-3; Transcript I at 122, 193-200, 264-267; Transcript II at 28-37, 72-74, 109-114.)

The next day, the Applicant was informed that his instructions resulted in a possible ordnance incident. In his own words, "And I at that point became very scared." (Transcript II at 35.)

At this time, the Applicant's Lead instructed the Applicant to update the Report to show what had happened concerning the work on the part after the Applicant had gone home. (Transcript I at 203-206, 255; Transcript II at 37-40.) In doing this, according to the Applicant, he noticed that the Report still had his instructions from the previous evening. As stated earlier, those instructions were superseded. The Applicant testified concerning his conduct at that time:

> All I did was delete that paragraph. Those four lines on the [Report] Screen to show the true course of events because that's what we always did was we dispositioned all our failures to show exactly what happened in the time sequence that they did happen. And that did not happen.[3] You know, in hindsight, I probably would have just put a parenthesis line below that, stating that the specific paragraph was not performed. But it was like drawing lines through a written Disposition and initialling (*sic*) it, except in this system, you couldn't draw lines through text. (Transcript II at 39-40.)

The Applicant further stated, "There would have been any number of ways to handle it other than the way I did. At the time, I thought I was just stating the true course of events. . . . At the time, I felt I wasn't - - there was no intent to defraud is the best I

[3] *See* Exhibit Y at 2.

can say." (Transcript II at 79.)[4] Finally, the Applicant printed up the new Report and replaced the ones from the prior night. He threw the old ones away. (Transcript II at 111-119.)[5]

Shortly afterwards, an investigation commenced into the Applicant's conduct with regards to the ordnance incident. This investigation continued until December 2005. On December 22, 2005, the Applicant was terminated from his employment with the Company, allegedly because of his conduct with regards to the ordnance incident. This termination had an effective date of January 2, 2006. (Government Exhibit 2; Applicant's Exhibit V; Transcript II at 80-88.)[6]

The Applicant was escorted from the Company's facility on December 22, 2005, and did not return there again. (Transcript at 88.) The Adverse Information Report states that the Applicant "was instructed to return company credit card and Secure ID for [remote computer access] since those items were at his home. He was instructed to have his spouse return them on 23 Dec 05, however, they were not returned until 3 Jan 06." (Government Exhibit 2.)

The Applicant disputes this version of events. He testified that he informed the Company that his wife, who also worked for the Company, would return the items on January 3, 2006. According to the Applicant, they were returned on that day. (Transcript II at 42-45, 86-87, 119-120.)

The Applicant admits that, during the period from December 22, 2005, to January 3, 2006, he obtained remote access to the Company's internal network. This was through the use of the Secure ID he was supposed to return. He further stated that, during this time, he sent personal email to co-workers and deleted what he describes as personal emails. He did not have authorization from anyone to access the system remotely. (Transcript II at 45-46, 69-71, 88-90, 121-122.)

The Company's IT Manager was authorized to access the Applicant's email account to capture any email sent or received after the date of his termination, December 22, 2005. In an email report, dated January 3, 2006, he states that "No e-mail messages were found in [the Applicant's Company] Exchange Sent, Deleted, Junk E-mail, Journal, Notes, Outbox, Sync, Search or Draft folders." (Government Exhibit 3 at 10.)

---

[4] *See* Transcript at 74-79.

[5] *See also* Transcript I at 238-241.

[6] Government Exhibit 2 is the Adverse Information Report submitted by the Company to the Government. Applicant's Exhibit V consists of the Applicant's copies of termination documents. The record does not contain any of the internal reports of the Company concerning any of the incidents involving the Applicant. It is noted that the documents in the record contain different dates of termination for the Applicant: January 2, 2006; January 3, 2006; and January 6, 2006. (*See* Transcript I at 5-9.)

The Applicant further admitted that, late on the afternoon of January 3, 2006, he accessed the Company's virtual private network for another reason. That is when he downloaded a copy of Applicant's Exhibit Y, the Report. He had no authorization from anybody to do this last event. In fact, the Applicant admitted that he did it in expectation of filing a law suit against the Company for wrongful termination. (Transcript at 90-93.)

Paragraph 3 (Guideline M - Misuse of Information Technology)

The Government alleges in this Paragraph that the Applicant is ineligible for clearance because he has used information technology in an inappropriate manner, thereby showing poor judgment, unreliability or untrustworthiness.

3.a. The Applicant's conduct as set forth in subparagraphs 2.b., 2.d., and 2.f., above, will be examined under this Guideline as well.

Mitigation

The Applicant is a highly educated, respected professional in his field. He has many years of experience in the defense industry, which is reflected in the many awards he has received for his work. (Applicant's Exhibit H.)

The current supervisor of the Applicant testified at the hearing. He has knowledge of the incidents concerning the Applicant at the Company. With that knowledge, he states, "I would recommend that the Security Clearance be granted. I have seen no indications of any issue at all in [the Applicant's] performance and ability to follow the rules and maintain the requirements for a Clearance." (Transcript I at 72.)

As stated earlier, the Applicant's Team Lead and his Manager from his time at the Company also testified on his behalf. They both testified that the Applicant is qualified to hold a security clearance. (Transcript I at 132, 210.)

The Applicant also submitted laudatory letters of reference from co-workers at his current employer (Applicant's Exhibits M and N), co-workers from his years at the Company (Applicant's Exhibits J, K, L, N, O, Q and U), as well as relatives and friends (Applicant's Exhibits R, S and T). He is described as someone with "personal integrity," who "always took his responsibilities seriously." One co-worker described the Applicant as "dependable, reliable, hard-working and conscientious." (Applicant's Exhibit L.) All of the letters are in this vein.

Policies

Security clearance decisions are not made in a vacuum. 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 considered 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, these guidelines are applied in conjunction with the factors listed in the adjudicative process. The administrative judge's overarching adjudicative goal is a fair, impartial, and commonsense 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. In addition, the administrative judge may also rely on his own common sense, as well as his knowledge of the law, human nature, and the ways of the world, in making a reasoned 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 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. Security clearance decisions include, by necessity, consideration of the possible risk that 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.

Finally, as emphasized by President Eisenhower in Section 7 of Executive Order 10865, "Any determination under this order . . . shall be a determination 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

Paragraph 1 (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*. (Emphasis supplied.)

The Applicant has three security violations over a period of three years, 2003, 2004 and 2005. I find that the following disqualifying conditions apply under Guideline K: ¶ 34(g) *any failure to comply with rules for the protection of classified or other sensitive information*; and ¶ 34(h) *negligence or lax security habits that persist despite counseling by management*.

There are three mitigating conditions that arguably apply to the Applicant's conduct under Guideline K. They are ¶ 35(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;* ¶ 35(b) *the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities;* and ¶ 35(c) *the security violations were due to improper or inadequate training*.

Concerning cases such as this, the DOHA Appeal Board has stated, "A person who has committed security violations has a very heavy burden of demonstrating that they should be entrusted with classified information. Because security violations strike at the heart of the industrial security program, an Administrative Judge must give any claims of reform and rehabilitation strict scrutiny." (ISCR Case No. 00-0030 (Appeal Board, September 20, 2001).) In the same case, the Appeal Board further says that the Government has a compelling interest in protecting classified information from disclosure to unauthorized persons, regardless of whether the disclosure is the result of deliberate or negligent conduct

The Applicant's conduct with the missing key can be put down to a parent's concern for a child. It obviously was an aberration from his normal procedure with regards to the key. Based on the state of the record, it has little if any security significance.

Concerning the classified photography, the evidence is mixed. Clearly, the procedures set out by the facility security officer in the reports of the Applicant's conduct do not comport with what his supervisors state the facts are. In addition, there was confusion about whether he actually did take any pictures of classified material. Based

on the state of the record, and acknowledging the Applicant's burden under this Guideline, I find that he has mitigated the security significance of his conduct. Paragraph 1 is found for the Applicant, as is subparagraph 2.a.

Paragraph 2 (Guideline E - Personal Conduct)

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

> Conduct involving questionable judgment, lack of candor, dishonesty or unwillingness to comply with rules or regulations can raise questions about an individual's reliability, trustworthiness and ability to protect classified information.

The entirety of the Applicant's conduct at the Company, as set forth under Paragraph 2, arguably brings into play disqualifying condition ¶ 16(c) under Guideline E: *credible adverse information in several adjudicative 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.*[7]

The following mitigating condition under Guideline E arguably applies to his conduct: 17(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*.[8]

The Applicant made serious errors in judgment with regards to the piece of classified hardware, how he worked on it, and what he did after he was terminated. Despite his protestations, and those of his witnesses, his employer of 27 years felt that his conduct was of a sufficient seriousness to justify termination. I need not decide whether his instructions with regards to the classified piece of hardware were correct or not. Rather, I find that his entire course of conduct, including after that event, shows extremely poor judgement, unreliability and untrustworthiness.

First, the Applicant changed the Report in an inappropriate manner. He states that nothing of importance was deleted, but I do not have his prior Report in the record and do not find him credible on this point. In reviewing the evidence, he knew that he was in trouble and I find that he amended the report to portray his conduct in the best possible light.

---

[7]As stated above, Subparagraphs 2.a. and 2.b. are found for the Applicant.

[8]For purposes of this Decision, I am viewing the term "offense" as including all of the actions of the Applicant. No criminal or dishonest conduct is implied to the Applicant in the use of this term.

Second, his post-termination conduct was completely inappropriate. He knew that he had been terminated and that he was no longer employed at the Company. The Applicant argues that the effective date was January 2, 2006. That is a thin reed to justify his conduct in remotely accessing the Company's computer system to clean up his email accounts and download Applicant's Exhibit Y. The Applicant admits that he had not asked permission from anyone to engage in this conduct.

I have considered the span of time that has passed since these events. While normally it would be mitigating, the Applicant continues to attempt to justify his conduct. I am not convinced that he would not act in the same way again if he felt that he was in the right. I must be convinced that the Applicant has truly changed his ways and will show good judgment, reliability, and trustworthiness with regards to all of his security responsibilities in the future. I am not so convinced. I find against the Applicant with regards to Guideline E.

Paragraph 3 (Guideline M - Misuse of Information Technology)

The security concern with regards to the Misuse of Information Technology is set out in AG ¶ 39:

> Noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual's reliability or trustworthiness, calling into question the willingness or ability to properly protect sensitive systems, networks, and information. Information Technology Systems include all related computer hardware, software, firmware, and data used for the communication, transmission, processing, manipulation, storage, or protection of information.

The Applicant's admitted conduct with regards to the Company's computer system provides support for the application of the following disqualifying conditions under Guideline M: ¶ 40(a) *illegal or unauthorized entry into any information technology system or component thereof;* ¶ 40(b) *illegal or unauthorized modification, destruction, manipulation or denial of access to information, software, firmware, or hardware in an information technology system;* ¶ 40(c) *use of any information technology system to gain unauthorized access to another system or to a compartmented area within the same system*; and ¶ 40(e) *unauthorized use of a government or other information technology system.*

The Applicant's conduct, as set forth above under subparagraphs 2.b. and 2.f., are cognizable under this paragraph as well.[9] I have examined the Applicant's explanations and find them wanting. Even though it has been several years since he engaged in this inappropriate conduct, I find that it continues to cast doubt on the Applicant's reliability, trustworthiness and good judgment. Accordingly, the mitigating condition set forth under ¶ 41(a) is not applicable.

[9]The facts set out under Subparagraph 2.b. do not have application under this Guideline.

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

I considered the potentially disqualifying and mitigating conditions in light of all the facts and circumstances surrounding this case. The Applicant is a hard-working, highly respected, and valuable member of the defense industry. I have carefully considered all the potential mitigating evidence in this case, including the laudatory personal opinions of his superiors and co-workers at the Company, and his current employer.

The Applicant, before and after his termination from the Company, acted inappropriately. In particular, he changed a report to lessen his culpability in a serious incident, and after his termination at least twice gained remote access to the Company's computer system for his own purposes. This is obviously serious conduct that he engaged in knowingly and voluntarily. Based on the current state of the record, I find that there is insufficient evidence of rehabilitation or other permanent behavioral changes. I also find that there is the likelihood of continuation or recurrence.

Overall, the record evidence leaves me with questions and doubts as to Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude the Applicant has not mitigated the security concerns arising from his inappropriate personal conduct and misuse of information systems.

On balance, it is concluded that the Applicant has not successfully overcome the Government's case opposing his request for a DoD security clearance. Accordingly, the evidence supports a finding against the Applicant as to the factual and conclusionary allegations expressed in Paragraphs 2 and 3 of the Government's Statement of Reasons. As stated above, Paragraph 1 is found for the Applicant.

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 THE APPLICANT
Subparagraph 1.a.:	For the Applicant
Subparagraph 1.b.:	For the Applicant
Subparagraph 1.c.:	For the Applicant
Paragraph 2, Guideline E:	AGAINST THE APPLICANT
Subparagraph 2.a.:	For the Applicant
Subparagraph 2.b.:	For the Applicant
Subparagraph 2.c.:	Against the Applicant
Subparagraph 2.d.:	Against the Applicant
Subparagraph 2.e.:	Against the Applicant
Subparagraph 2.f.:	Against the Applicant
Paragraph 3, Guideline M:	AGAINST THE APPLICANT
Subparagraph 3.a.:	Against the Applicant

Conclusion

In light of all of the circumstances presented by the record in this case, it is not clearly consistent with the national interest to grant Applicant eligibility for a security clearance. Eligibility for access to classified information is denied.

WILFORD H. ROSS
Administrative Judge