DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 06-24224
SSN:	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: James F. Duffy, Esquire, Department Counsel
For Applicant: *Pro Se*

January 16, 2008

Decision

HOGAN, Erin C., Administrative Judge:

Applicant submitted his Security Clearance Application (SF 86), on March 17, 2006. On September 10, 2007, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) detailing the security concerns under Guidelines E and M for Applicant. 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 acknowledged receipt of the SOR on September 13, 2007. He answered the SOR in writing on September 21, 2007, and requested a decision on the written record. DOHA received the request on September 26, 2007. Department Counsel submitted a File of Relevant Material (FORM) on October 31, 2007. Applicant received a copy of the FORM on November 6, 2007. He responded to the FORM on November 18, 2007. The FORM as well as Applicant's response to the FORM was forwarded to the hearing office on November 30, 2007. I received the case assignment

on December 10, 2007. Based upon a review of the case file, pleadings, and exhibits, eligibility for access to classified information is denied.

Findings of Fact

In his Answer to the SOR, dated September 21, 2007, Applicant denied all the allegations.

Applicant is a 54-year-old employee of a defense contractor seeking to maintain a security clearance. He submitted a security clearance application on March 17, 2006.[1] He has held a security clearance since 1989.[2]

In March 2003, Applicant was hired by a defense contractor to work on a program which provided television services to military ships at sea. The company was a subcontractor to the main company who was awarded the contract.[3]

In March 2005, the company encountered a funding issue with the government. On March 2, 2005, Applicant's program manager sent out an e-mail indicating that until funding was in place all communications with the government customer should be filtered through him or the main contractor.[4]

In March/April 2005, Applicant's program manager became suspicious of Applicant's "over-involved" interaction with the government employees who worked on the contract. He received approval to search Applicant's e-mail activity on the office server. The initial review of Applicant's e-mail provided nothing substantive but the program manager continued to monitor his work e-mail.[5]

On March 17, 2005, Applicant's wife sent the program manager an e-mail on Applicant's work e-mail account accusing him of lacking compassion pertaining to a knee injury Applicant suffered.[6] This raised an issue about her unauthorized use of the company e-mail system. Applicant explained in his response to the FORM that he was checking his e-mail while at home on sick leave. His wife was there when he was reviewing his e-mails and became upset about his program manager's lack of sympathy

[1] Item 5.

[2] Item 5.

[3] Item 8.

[4] Item 7 at 6.

[5] Item 7 at 3-4.

[6] Item 7 at 9.

for his medical condition which resulted in her sending an e-mail to the program manager on Applicant's business e-mail account.[7]

The program manager continued to review Applicant's e-mail. He discovered that on June 1, 2005, Applicant sent a training guide that was not finalized to the government employees who were working on the contract. The rule that all communications with the government customer should be filtered through the program manager or the principal contractor was still in effect. Applicant sent additional items of information to the government customer without authorization. The items included information that management considered proprietary information belonging to the main contractor and another company. The release of this information made Applicant's company vulnerable to litigation. Applicant also made several disparaging comments in the e-mails sent to the government customer about his boss (the program manager) and the main contractor.[8]

On June 13, 2005, Applicant's employer terminated him for 1) insubordination and willful disobedience of assignments and/or orders; 2) disclosure of company processes and records that originated due to the company's development and production; 3) removal of company records without authorization; 4) break of confidentiality to the company, his supervisor and co-workers as well as other contractors involved in the program; and 5) conflict of interest.[9]

On the same day that he was terminated, Applicant called the program manager of the government agency who Applicant worked with on the contract. She advised him to wait for a phone call. He received a phone call from another defense contractor and was hired by that defense contractor the same day. Although he was completely shocked about the basis for his termination, he did not rebut the charges because he had obtained new employment.[10] He indicated in his response to the FORM that the program manager of the government customer did not want to lose access to this technical expertise.

In his response to the SOR, dated September 21, 2007, Applicant maintains that he did not release proprietary information to the government customer. He claims that the technical manual and training guide were government property and that his former employer had no claim to them. Any work provided by his former employer was performed with products developed by the system's original equipment manufacturer. He also claims that his supervisor and the principal contractor were aware of any e-mails sent to the government customer because they were copied on any e-mail transmissions related to the contract. Applicant did not provide additional documentation

---

[7] Response to FORM, dated November 18, 2007.

[8] Item 7.

[9] Item 6.

[10] Item 8.

verifying that he sent copies of the items sent to the government agency to his program manager and the main contractor. The e-mails the company attached to the termination memorandum do not show Applicant sent copies to his supervisor and the main contractor.[11] In fact, Applicant blind copied the program manager of the government customer on e-mail correspondence that he sent to the main contractor.[12]

Applicant disputes the conflict of interest allegation. He states that he held no other jobs and his work consisted solely of the work assigned to him as part of the subcontract.[13]

In his response to the FORM, dated November 18, 2007, Applicant states that it was his first opportunity to review a copy of the program manager's memorandum which outlines the basis for Applicant's termination. He claims that any proof that he would need to counter these allegations was contained in his company e-mail account, which, he no longer has access to because of his termination. He claims that the main contractor instructed him to send the training documents back to the government customer via e-mail and that he copied both the main contractor and his program manager on the e-mail transmissions. He states that claims of disseminating another company's proprietary information is false. He states the information came from the company's manual and that the government customer's engineers have access to all equipment for the program. Anyone with access to the equipment has the ability to open the equipment and document the wiring of the cards and/or interconnection within the equipment. He states this is a standard trouble-shooting procedure when dealing with system problems on board ships. He believes that his former program manager has treated him unfairly since November 2004, after he suffered from a heart attack. He provided the name and number of the government employee he worked closely with on the contract. He claims that she will verify that he was the sole source of system expertise which is why she made an effort to find him another job with a company that she would have access to his knowledge.[14]

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 useful in evaluating an Applicant's eligibility for access to classified information.

---

[11] Item 7 at 6-26.

[12] Item 7 at 13.

[13] Item 4.

[14] Response to FORM, dated November 18, 2007.

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 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.

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. 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." *See also* EO 12968, Section 3.1(b) (listing multiple prerequisites for access to classified or sensitive information).

Analysis

Guideline E, Personal Conduct

The Government established a prima facie case under Guideline E, Personal Conduct. The overall security concern relating to the Personal Conduct guideline 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 tor provide truthful and candid answers during the security clearance process or any other failure to cooperate with the security clearance process.

The guideline notes several conditions that could raise security concerns. PC DC ¶ 16(d) (*credible adverse information that is not explicitly covered under any other single guideline, 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; (3) a pattern of dishonesty or rule violations*) applies to Applicant's case.

The government established a prima facie case that Applicant was terminated from his employment with a defense contractor in June 2005 for insubordination or willful disobedience of assignments or orders; disclosure of company processes and records that originated due to the company's development and production; removing company records without authorization; breach of confidentiality to his company, his supervisor, co-workers and other contractors working on the contract; and conflict of interest.

The record evidence establishes that Applicant willfully disobeyed his program manager's order to filter any communications with the government contractor through the program manager or the main contractor. Applicant forwarded the training manual he was working on directly to the government customer without consulting with the program manager or the main contractor. Applicant maintains that he copied the program manager and the main contractor when e-mailing the documents to the government customer but has provided nothing to verify this action. Even if he did so, the order directs that employees contact the program manager or main contractor **before** communicating or sending information to the government contractor. Even if he copied the program manager and the main contractor in his e-mail, he still did not follow the terms of the order. Applicant did not coordinate with them prior to sending the document. It is clear from the program manager's memorandum outlining the cause for termination that the order was still in effect at the time Applicant forwarded the information to the government contractor.

Applicant's blind copying the government customer on certain e-mail transmissions that he sent to the main contractor is a breach of confidentiality. The disclosure of company processes and records allegation relates to the information sent to the government customer about another contractor's proprietary information pertaining to the development of the product. Although Applicant maintains the

information was not proprietary, his former employer thought otherwise. Aside from his own assertions, he provided no documents verifying that the information was not considered proprietary by the company who developed the product.

The guideline also includes examples of conditions that could mitigate security concerns arising from personal conduct. Two Personal Conduct Mitigating Conditions (PC MC) are potentially applicable to Applicant's case. PC MC ¶ 17c (*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*) does not apply. Applicant's company considered his conduct so serious that it warranted termination. The company was particularly concerned about their vulnerability to being sued by the main contractor and the other company whose proprietary information was released without authorization. The e-mail communications reveal that Applicant had little respect for the program manager and the main contractor. His disparaging comments about his superiors in e-mails with the government customer demonstrate poor judgment. Blind copying e-mail communications sent to the main contractor to the government customer raises issues about his trustworthiness. Applicant was terminated from employment in 2005. It is too soon the conclude that sufficient time has passed to indicate that Applicant's conduct no longer raises doubts about his reliability, trustworthiness, and good judgment.

PC MC ¶ 17(d) (*the individual has acknowledged the behavior and obtained counseling to change the behavior or taken other positive steps to alleviate stressors, circumstances, or factors that caused untrustworthy, unreliable, or other inappropriate behavior, and such behavior is unlikely to recur*) does not apply. Applicant maintains that he did nothing wrong and therefore has taken no steps to rectify his past conduct. While he has several explanations for his conduct, he provided no corroborating evidence to support his assertions.

The government established a prima facie case raising security concerns under personal conduct. As such, Applicant has the ultimate burden of persuasion as to obtaining a favorable clearance decision.[15] Applicant has not met that burden.

Guideline M, Use of Information Technology Systems

The government did not establish a prima facie case under Guideline M. The security concern under Guideline M is set in AG ¶ 39:

> Noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual's reliability and trustworthiness, calling into question the willingness or ability to properly protect sensitive systems, networks and information. Information Technology Systems include all related computer

[15] Directive, ¶ E3.1.15.

> hardware, software, firmware, and data used for the communication, transmission, processing, manipulation, storage, or protection of information.

There is nothing in the record evidence that indicates Applicant misused the information technology systems. No rules, procedures, guidelines or regulations pertaining to the company information technology systems were included in the record which would raise questions pertaining to Applicant's reliability and trustworthiness with regard to the protection of sensitive systems, network and information. While there was one occasion where Applicant's wife sent his program manager an e-mail from Applicant's company e-mail account complaining about the program manager's lack of compassion pertaining the Applicant's medical condition, there is nothing else which indicates Applicant misused or manipulated the company's information technology systems. Granted, Applicant did not demonstrate the best judgment in allowing his wife to send the program manager an e-mail on his business account, however, there were no other instances where his wife used Applicant's company e-mail. Considering the company was monitoring Applicant's e-mail, they would have discovered further e-mails if she had. Guideline M is found for Applicant.

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) 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 commonsense 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. Applicant was a mature adult at the time he committed the conduct which was the basis for his termination. His conduct was unprofessional and he fails to acknowledge any wrongdoing and/or provide evidence supporting his assertions that he did not disobey company orders, breach company confidentiality, or disclose another company's proprietary information without authorization. He provided minimal information about his current employment situation.

Overall, the record evidence leaves me with questions or doubts as to Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude

Applicant did not mitigate the security concerns arising under the personal conduct guideline.

Formal Findings

Formal findings for or against Applicant on the allegations set forth in the SOR, as required by section E3.1.25 of Enclosure 3 of the Directive, are:

Paragraph 1, Guideline E:	AGAINST APPLICANT
Subparagraph 1.a:	Against Applicant
Paragraph 2, Guideline M:	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 not clearly consistent with national security to grant Applicant eligibility for a security clearance. Eligibility for access to classified information is denied.

ERIN C. HOGAN
Administrative Judge