DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
----------	)	
SSN: ----------	)	ISCR Case No. 07-06332
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Eric Borgstrom, Esquire, Department Counsel
For Applicant: Alan V. Edmunds, Esquire

February 6, 2008

Decision

MALONE, Matthew E., Administrative Judge:

On October 4, 2006, Applicant submitted an Electronic Questionnaire for Investigations Processing (e-QIP) to request a security clearance for his employment with a defense contractor. After reviewing the results of the ensuing background investigation, adjudicators for the Defense Office of Hearings and Appeals (DOHA) were unable to make a preliminary affirmative finding[1] that it is clearly consistent with the national interest to grant Applicant's request. On July 27, 2007, DOHA issued to Applicant a Statement of Reasons (SOR) alleging facts which raise security concerns addressed in the Revised Adjudicative Guidelines (AG)[2] under Guideline M (misuse of information technology) and Guideline E (personal conduct).

[1] Required by Executive Order 10865, as amended, and by DoD Directive 5220.6 (Directive), as amended.

[2] Adjudication of this case is controlled by the Revised Adjudicative Guidelines, approved by the President on December 29, 2005,which were implemented by the Department of Defense on September 1, 2006. Pending official revision of the Directive, the Revised Adjudicative Guidelines supercede the guidelines listed in Enclosure 2 to the Directive, and they apply to all adjudications or trustworthiness determinations in which an SOR was issued on or after September 1, 2006.

Applicant timely responded to the SOR, denied all of the allegations therein, and requested a hearing. The case was assigned to me on September 10, 2007, and I scheduled a hearing to be held on December 17, 2007.[3] The parties appeared as scheduled. The government presented six exhibits (Gx. 1 - 6) and one witness. Applicant testified in his own behalf, offered 22 exhibits (Ax. A - V), and presented one witness. DOHA received the transcript (Tr.) on January 7, 2008. Based upon a review of the case file, pleadings, exhibits, and testimony, Applicant's request for a security clearance is denied.

Findings of Fact

Under Guideline M, the government alleged in SOR ¶ 1.a that Applicant received two written reprimands in May 2006 for not providing his employer the source codes and other information needed to run a computer program Applicant had developed for contract he was working on for his employer. In SOR ¶ 1.b, the government alleged Applicant included an expiration routine in the same computer program that was not requested by his employer. In SOR ¶ 1.c, the government alleged Applicant deleted a source code for the same computer program.

Under Guideline E, the government alleged in SOR ¶ 2.a the same information alleged in SOR ¶ 1.a. In SOR ¶ 2.b, the government alleged that, by withholding the information needed to run the program referenced in SOR ¶ 1, Applicant violated a Patent and Trade Secret agreement he signed when he was hired in March 2005. After a thorough review of the pleadings, transcript, and exhibits, I make the following findings of fact.

Applicant is 35 years old. Since October 2007, he has worked as a senior software engineer for a defense contractor in support of a joint U.S. military effort in Iraq. In 2003, he graduated from college with a degree in B.S. in computer science. Thereafter, he worked as a software engineer until being hired by a different defense contractor for work on a U.S. Army contract in Iraq from March 2005 until leaving that job in May 2006. Applicant was hired for work as an information technology (IT) technician. In April 2005, after a brief training program, Applicant was sent to work in Iraq location. His company provided facilities maintenance, repair, and other services required by the U.S. Army. Applicant was responsible for installation, support, and maintenance of various communications and IT equipment and systems.

On March 29, 2005, when Applicant was hired, he signed a "Patent and Trade Secret Agreement." The agreement states provides that, as a condition of his employment, Applicant agreed "to disclose promptly to the Company all inventions, discoveries and improvements made by [Applicant] during [his] employment," and that "any and all notes, tapes, discs, fiche, film, records and drawings made or kept by [Applicant] of the work performed in connection with [his] employment or in relation to

[3] Applicant was unavailable for a more timely hearing, because he was assigned to his company's work site in Iraq.

any of said inventions, discoveries or improvements, were and are the sole property of the Company." (Gx. 3, Tab A)

About a month after Applicant arrived in Iraq, he offered to improve an internal tracking and reporting data base his company used to manage tasks required of them by the Army. For example, a request would come in for the company to fix something at a building in Baghdad. That request would be put into the data base with a date assigned and date due for completion. The company would use the data base to help manage its resources and track the progress of its tasks when reporting to the Army about its efforts. Applicant told his managers he could create a program that would be more robust and, thus, more useful in that effort. Applicant spent about a month writing the code and assembling the software needed to create the program. By all accounts, the program proved very useful to Applicant's company.

Applicant placed in the program a code that would cause the program to expire sometime in April 2006. The expiration code was not requested by his company. Applicant explained that, in building the data base program, he had used parts of other programs he had built while in school or at earlier jobs, and the expiration code was already included with some of those parts. Applicant also assigned a password to the program, which he initially kept to himself. Applicant also kept to himself the source codes, which provide a measure of security so that only the programmer or other authorized persons may access the program to modify or repair it.

As a result of a 1992 accident in which he suffered a severe head injury, Applicant has had a disability that impairs his speech and mobility. He is not at all cognitively impaired, but his condition manifests itself in speech and coordination challenges similar to those exhibited by persons with cerebral palsy. Beginning in late 2005, Applicant began having trouble with his managers, as he felt they were discriminating against or harassing him because of his physical disabilities. On March 9, 2006, he filed a complaint using the Government Accountability Office's (GAO) Fraud Net web site. He alleged various acts of discrimination and harassment, as well as racial discrimination and harassment of minority co-workers. He also alleged various acts of waste, fraud, abuse, and misconduct by his supervisors.

Applicant testified that his claims are still being investigated by GAO. However, on September 26, 2006, a Department of the Army investigation of his complaints concluded there was no basis for Applicant's allegations of wrongdoing by his supervisors. (Gx. 3, Tab D)

On April 24, 2006, the expiration code caused the data base to stop working. A message appeared stating that the "program trial period" had expired and referred the user to Applicant. At the time this occurred, he was not available and no one else had the source codes or passwords needed to access the program to effect repairs. Applicant was eventually located and he fixed the immediate problem. However, this event made clear to his supervisors that they needed the codes and passwords to avoid such problems in the future.

In a meeting on April 26, 2006, Applicant was asked to remove the expiration code and to provide all information (codes, passwords, software, etc.) necessary for the company to manage the program without having to rely on one person to solve problems. Applicant refused to provide the information, becoming upset and belligerent over the request. He demanded compensation for the program and claimed he was owed back overtime pay by the company. At one point, because he was angry about his circumstances at the company, he deliberately deleted a folder containing the source codes for the program. He was able to reconstruct the codes over the next ten days. On April 28, 2006, Applicant was told he would be terminated for his refusal to comply with the company's requests; however, a written notice of termination was not signed or acted on.

Applicant was twice reprimanded in May 2006 for his behavior in the workplace and for his refusal to provide the program information. Also in May 2006, Applicant was notified he would be let go as part of a reduction in force that also affected about 60 other employees. Applicant eventually provided some of the information requested, but only after he was reminded of the Patent and Trade Secret Agreement he had signed. His employer also intended to withhold a performance bonus due to Applicant if he did not comply with their requests.

Applicant's last day in Iraq was May 12, 2006, and he ended his employment with the company on May 17, 2006. On May 26, 2006, the data base program crashed and the company had to resort to a manual tracking system. A subsequent review estimated the cost of Applicant's actions and the labor required to restore or recreate the functional equivalent of the automated tracking system at about $190,000. (Gx. 3, Tab C)

After he was laid-off, Applicant filed a complaint with the Department of the Army Inspector General. He alleged he was terminated from his employment in reprisal for his earlier complaint to GAO. On April 17, 2007, the Army Inspector General concluded there was no reprisal, as Applicant's "termination was based on ... reduced manpower requirements... and [Applicant's] documented unprofessional conduct." (Gx. 6)

Applicant's record at the company where he has worked since October 2006 is excellent. Several government, military, and company associates and superiors have lauded his efforts and expertise. His performance appraisals reflect superior work and a great deal of potential for continued success. (Ax. A - V)

Policies

Each security clearance decision must be a fair, impartial, and commonsense determination based on examination of all available relevant and material information, and consideration of the pertinent criteria and adjudication policy in the Revised Adjudicative Guidelines (AG).[4] Decisions must also reflect consideration of the factors

[4] Directive. 6.3.

listed in ¶ 2(a) of the new guidelines.[5] The presence or absence of a disqualifying or mitigating condition is not determinative of a conclusion for or against an applicant. However, specific applicable guidelines should be followed whenever a case can be measured against them as they represent policy guidance governing the grant or denial of access to classified information. In this case, the pleadings and the information presented by the parties require consideration of the security concerns and adjudicative factors addressed under Guideline M (misuse of information technology systems), at AG ¶ 39, and Guideline E (personal conduct) at AG ¶ 15.

A security clearance decision is intended to resolve whether it is clearly consistent with the national interest[6] for an applicant to either receive or continue to have access to classified information. The government bears the initial burden of producing admissible information on which it based the preliminary decision to deny or revoke a security clearance for an applicant. Additionally, the government must be able to prove controverted facts alleged in the SOR. If the government meets its burden, it then falls to the applicant to refute, extenuate or mitigate the government's case. Because no one has a "right" to a security clearance, an applicant bears a heavy burden of persuasion.[7] A person who has access to classified information enters into a fiduciary relationship with the government based on trust and confidence. The government, therefore, has a compelling interest in ensuring each applicant possesses the requisite judgement, reliability and trustworthiness of one who will protect the national interests as his or her own. The "clearly consistent with the national interest" standard compels resolution of any reasonable doubt about an applicant's suitability for access in favor of the government.[8]

Analysis

Misuse of Information Technology Systems.

Under Guideline M, "[n]oncompliance 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 hardware, software, firmware, and data used for the communication, transmission, processing, manipulation, storage, or protection of information." (AG ¶ 39). The government presented sufficient information

---

[5] Commonly referred to as the "whole person" concept, these factor are:(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.

[6] *See Department of the Navy v. Egan*, 484 U.S. 518 (1988).

[7] *See Egan,* 484 U.S. at 528, 531.

[8] *See Egan;* Revised Adjudicative Guidelines, ¶ 2(b).

to support the allegations in SOR ¶¶ 1.a, 1.b, and 1.c. The latter two allegations simply plead supporting evidence, and are not, by themselves, disqualifying. However, taken together with SOR ¶ 1.a, they address the gravamen of this case; namely, the security ramifications of Applicant's apparent willingness to deny access to a computer program needed by his employer and, more importantly, by the U.S. Army. Further, the information presented requires consideration of the disqualifying condition listed at AG ¶ 40(b) (*illegal or unauthorized modification, destruction, manipulation or denial of access to information, software, firmware, or hardware in an information technology system*) (emphasis added).

In response to the SOR, Applicant has argued for a different interpretation of the information in Gx. 3. He insists he did nothing wrong in managing the program, that he was the victim of harassment and discrimination, and that the information presented should be viewed as his former employer's way of getting even with him for his GAO complaints. However, in weighing the available information, I am more persuaded by the e-mails and correspondence in Gx. 3 that was generated at or near the time of the events in question than I am by Applicant's more current interpretation of those same events. To accept Applicant's argument is to conclude, which I do not, that the authors of those e-mails and other correspondence had in mind an organized effort to get back at him. The more plausible interpretation of this information is that, because Applicant was frustrated with his circumstances, he used the program he had developed as leverage against his employer, who he felt had mistreated him and denied him proper compensation.

The record does not support consideration of any of the Guideline M mitigating conditions listed in AG ¶ 41. This conduct was recent and Applicant has not demonstrated how his actions do not reflect adversely on his "reliability, trustworthiness, or good judgment." (AG ¶ 41(a)) Indeed, his actions show a willingness to use his technical expertise to protect his own interests, even at the expense of the government's war effort. Nor does the record show Applicant's conduct constituted a minor transgression (AG ¶ 41(b)). The estimated damage from Applicant's actions was nearly $200,000. Finally, his conduct was not unintentional or inadvertent. Rather than try to correct the situation, Applicant only partially complied with his employer's requests after being threatened with termination. (AG ¶ 41(c)). Applicant's information about what may or may not have occurred in the workplace is insufficient to mitigate the security concerns about his conduct.

Personal Conduct.

The security concern about Applicant's personal conduct, as expressed in the AG ¶ 15, is that "[c]onduct 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." Applicant may not be disqualified under Guideline E for the SOR ¶ 2.a allegation. While the record shows he misused information technology systems as alleged, such conduct is specifically covered under Guideline M and must be addressed according to AG ¶ 40(b), as discussed above.

As to SOR ¶ 2.b, available information requires consideration of the disqualifying conditions listed in AG ¶ 16(f) (*violation of a written or recorded commitment made by the individual to the employer as a condition of employment*). Applicant tried to renege on a written agreement he signed when he was hired. That agreement addressed his employer's interest in any work product generated by its employees while engaged in its business and using its resources. It was clearly a condition of his employment. Applicant tried to evade its restrictions and would surely have done so had his employer not insisted on trying to enforce the agreement so the program Applicant had constructed could continue to be used to support the government. For the same reasons discussed under Guideline M, above, the record does not warrant consideration of any of the mitigating conditions listed under AG 17.

Whole Person Concept.

I have evaluated the facts presented in this record and have applied the appropriate adjudicative factors, pro and con, under Guidelines M and E. I have also reviewed the record before me in the context of the whole person factors listed in ¶ AG 2(a).[9] Applicant is a mature adult whose recent job performance has been exemplary. However, the positive information about Applicant is insufficient to overcome the adverse information about his conduct at his previous job. Because access to classified information is increasingly intertwined with automated information technology systems, deliberately impeding the government's ability to use those systems in support of the national interest is conduct that has significant security ramifications. This is especially so when assessing the suitability of one who has access by virtue of his technical expertise. Despite Applicant's recent conduct, doubts persist about whether, if his circumstances again turn sour, he will again try to leverage his technical expertise for his own interests. Because protection of the national interest is paramount in these determinations, such doubts must be resolved in favor of the national interest.[10]

[9] *See* footnote 5, *supra.*

[10] *See* footnote 8, *supra.*

Formal Findings

Formal findings 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 M:	AGAINST APPLICANT
Subparagraph 1.a:	Against Applicant
Subparagraph 1.b:	Against Applicant
Subparagraph 1.c:	Against Applicant
Paragraph 2, Guideline E:	AGAINST APPLICANT
Subparagraph 2.a:	For Applicant
Subparagraph 2.b:	Against Applicant

Conclusion

In light of all of the foregoing, 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.

MATTHEW E. MALONE
Administrative Judge