DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 08-00162
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Robert E. Coacher, Esquire, Department Counsel
For Applicant: *Pro Se*

October 21, 2009

Decision

CREAN, Thomas M., Administrative Judge:

Applicant submitted his Electronic Questionnaire for Investigations Processing (e-QIP) as part of his employment with a defense contractor on May 5, 2007 (Item 4). On June 3, 2009, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) detailing security concerns under Guidelines M (Use of Information Technology Systems) and Guideline E (Personal Conduct) (Item 1). 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 June 10, 2009 (Item 2).

Applicant answered the SOR in writing on June 24, 2009. He admitted all the allegations with explanation, and elected to have the matter decided on the written record in lieu of a hearing (Item 3). Department Counsel submitted the government's written case on July 20, 2009. Applicant received a complete file of relevant material

(FORM) on August 5, 2009, and was provided the opportunity to file objections and submit material to refute, extenuate, or mitigate the security concerns by September 16, 2009. Applicant timely submitted additional information. The case was assigned to me on September 21, 2009. Based upon a review of the case file and the pleadings, eligibility for access to classified information is denied.

Findings of Fact

Applicant admitted the factual allegations under Guidelines M and E. The allegation under Guideline M involves the use of a company computer to access, view, and download pornographic material in violation of company policy. The Guideline E violations include use of the company computer to access pornographic material in violation of company policy, the use of marijuana between September 1996 and December 2000, and a state tax lien placed against him in June 1998. I thoroughly and carefully reviewed the case file and the pleadings. I make the following findings of fact.

Applicant is 35 years old and a security consultant for a defense contractor. He has worked in various capacities as a security consultant in the defense industry for over five years. He was granted access to classified information in 2005, but his access was revoked in May 2006. It appears from the file that he may have been granted interim access to classified information after 2006. He is married with at least one child. He served four years on active duty in the Navy and received an Honorable Discharge (Item 4, e-QIP).

Applicant was a facility security officer for a defense contractor in May 2006, when pornographic material was found on his computer. His company's policy prohibits accessing and downloading pornographic material using a company computer. Applicant was immediately terminated from his position as the facility security officer (Items 5 and 6). Applicant admits the conduct but feels he has been sufficiently punished. He feels he is not a threat to national security and has been punished enough. Applicant may have been granted interim access to classified information by another defense contractor within a month of being terminated by his previous employer. He has continued to work in security since June 2006, been promoted, received raises, and advanced to a senior security specialist. In this capacity, he has advised and assisted other government agencies with security issues. Applicant stated his worst problem concerning the pornographic material was telling his wife. However, she has been supportive. (Response to FORM, received DOHA September 8, 2009).

Applicant admitted that he failed to file a state income return for tax year 1998. Applicant completed his federal and state tax returns as normal. He thought he had mailed both forms. He received a federal tax refund and thought he had received his state tax refund. When he was advised by the state that he had not filed the return, he looked for his return to verify it had been filed. Instead, he found his state tax return still in the envelope in the file ready for mailing. Applicant mailed his state tax return, paid the penalties, and the debt is resolved (Response to FORM, received DOHA September 8, 2009).

Applicant admitted using marijuana about 20 times from September 1996 until December 2000. Applicant was in his early 20s at the time. He has not used marijuana since January 2003, and regrets the use of marijuana while he was a young man. He also was concerned because his father used drugs during the Vietnam era and recently died of throat cancer (Response to SOR, dated June 24, 2009; Response to Form, received DOHA, September 8, 2009).

Applicant informed his wife of his conduct concerning pornography and the reasons he was terminated. He uses himself as an example when he teaches classes as a security consultant of the security consequences of drug abuse and misuse of information technology. He is involved in community activities of his homeowners' association and neighborhood watch. He is also more active in his church. The facility security officer (FSO) for one of the companies he advises noted that Applicant is a professional dedicated to his work. He does not question Applicant's loyalty and does not consider Applicant a danger with managing classified information. Applicant has ensured that the facility security officer's company stays in compliance with security requirements. He discussed Applicant's prior conduct with him and he is convinced that Applicant's inappropriate conduct will not happen again (Response to FORM, received DOHA September 8, 2009).

Policies

When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the revised Administrative Guidelines. 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.

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.

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. 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.

Analysis

Guideline M, Use of Information Technology Systems

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 (AG ¶ 39). Applicant's conduct in accessing, viewing, and downloading pornographic material on a company computer in violation of company policy raises Information Technology Disqualifying Condition (IT DC) ¶ 40(e) (unauthorized use of a government or other information technology system).

I considered Information Technology Mitigating Conditions (IT MC) AG ¶ 41 (a) (so much time has elapsed since the behavior happened or it happened under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment); IT MC AG ¶ 41 (b) (the misuse was minor and done only in the interest of organizational efficiency and effectiveness, such as letting another person use one's password or computer when no other timely alternative was readily available); and IT MC AG ¶ 41(c) (the conduct was unintentional or inadvertent and was followed by a prompt, good-faith effort to correct the situation and by notification of supervisor). I find that none of the mitigating conditions apply. Applicant deliberately accessed, viewed, and downloaded pornography on his company computer in 2006. He was then the facility security officer responsible for the company's compliance with security procedures and its security posture. It was done for his own gratification and not to advance any company programs or issue. This breach of the technology system in violation of company policy is even more serious since Applicant was the company facility security officer. It was his duty to ensure the security worthiness of his company and the proper use of their computer systems. I find against Applicant as to Guideline M.

Guideline E, Personal Conduct

A security concern is raised because conduct involving questionable judgment, untrustworthiness, unreliability, or unwillingness to comply with rules and regulations can raise questions about an individual's reliability, trustworthiness, and ability to protect classified information (AG ¶ 15). Personal conduct is always a security concern because it asks the central question does the person's past conduct justify confidence the person can be entrusted to properly safeguard classified information.

Applicant's downloading of pornographic material in violation of company policy, his use of marijuana, and his failure to file a state income tax return raises Personal Conduct Disqualifying Conditions (PC DC) AG ¶ 16(c) (credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any 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 safe guard protected information); PC DC AG ¶ 16(d) (credible adverse information that is not explicitly covered under any other guideline and may not be sufficient by itself for an adverse determination, 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: (3) a pattern of dishonesty or rule violations); and PC DC AG ¶ 16(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). This type of conduct, whether known or not, involves questionable judgment, untrustworthiness, unreliability, or unwillingness to comply with rules and regulations. These events raise concerns about Applicant's reliability, trustworthiness, and ability to protect classified information.

I have also considered Personal Conduct Mitigating Conditions (PC MC) AG ¶ 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); and PC MC AG ¶ 19(e) (the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress). Much time has passed since Applicant used marijuana. He has not used the drug since January 2003, over six years ago. His last use happened a long time ago and there has been an appropriate period of abstinence. His past marijuana use is unlikely to recur and does not now cast doubt on his trustworthiness or reliability. His failure to file a state tax return was a one-time inadvertent occurrence. I find that Applicant mitigated the security concerns about his failure to file a state tax return and marijuana use.

However, Applicant misuse of information technology systems in violation of company policy has not been mitigated. He used his company computer in violation of

company policy prohibiting download of pornographic material. This is a serious breach of company policy as well as personal conduct that is questionable and shows an unwillingness to comply with rules and regulations. This conduct occurred in 2006, only three years ago. Applicant was then his company's facility security officer. He knew and understood the ramifications of his conduct for his security clearance. Knowing this, he still accessed, viewed, and downloaded pornographic material. This offense happened recently and is serious. It can recur at any time and at the stroke of a computer key. I find against Applicant as to Personal Conduct.

"Whole Person" Analysis

Under the whole person concept, the administrative judge must evaluate an applicant's security eligibility by considering the totality of the applicant's conduct and all the circumstances. An 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 a security clearance must be an overall commonssense judgment based upon careful consideration of the guidelines and the whole person concept.

Applicant has not established that he is trustworthy, reliable, and exercises good judgment. To the contrary, his accessing, viewing, and downloading pornographic material on a company computer when he was the facility security officer is a strong indicator that he will be untrustworthy, unreliable, and use poor judgment in the management of classified material. He has established that his past use of marijuana and his inadvertent failure to file a state tax return in 1998 is not of security significance. The record evidence leaves me with questions about Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude Applicant has not mitigated the security concerns arising from his misuse of technology information systems 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 H:	AGAINST APPLICANT
Subparagraph 1.a:	Against Applicant
Paragraph 2, Guideline E:	AGAINST APPLICANT
Subparagraph 2.a:	Against Applicant
Subparagraph 2.b:	For Applicant
Subparagraph 2.c:	For 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.

_____
THOMAS M. CREAN
Administrative Judge