DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 09-03471
SSN:	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Julie R. Mendez, Esquire, Department Counsel
For Applicant: *Pro se*

_____

Decision

_____

HOGAN, Erin C., Administrative Judge:

Applicant submitted a Questionnaire for National Security Positions on April 16, 2008. On November 19, 2009, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) detailing security concerns under Guideline E, Personal Conduct, and Guideline M, Use of Information Technology Systems. 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 adjudicative guidelines (AG), effective within the Department of Defense for SORs issued after September 1, 2006.

On December 9, 2009, Applicant answered the SOR and requested a hearing before an administrative judge. Department Counsel was ready to proceed on February 17, 2010. The case was assigned to me on February 19, 2010. On March 11, 2010, a Notice of Hearing was issued, scheduling the hearing for April 15, 2010. The case was heard on that date. The Government offered five exhibits which were admitted as Government Exhibits (Gov) 1 – 5. Applicant testified and submitted no documents. The record was held open until April 22, 2010, to allow Applicant to submit additional documents. He timely submitted three documents which were admitted as Applicant Exhibits (AE) A – C. Department Counsel's responses to AE A – C are marked as Hearing Exhibits (HE) II – IV. The transcript (Tr.) was received on April 27, 2010. Based

upon a review of the case file, pleadings, exhibits, and testimony, eligibility for access to classified information is granted.

Procedural Issues

Applicant requested that his case be decided on the administrative record. Department Counsel converted Applicant's case to a hearing pursuant to paragraph E3.1.7 of the Directive. The documents related to this action are marked as Hearing Exhibit I.

Findings of Fact

In his Answer to the SOR, Applicant denied the overall concerns raised under the personal conduct and use of information technology guidelines but admitted the underlying factual SOR allegations.

Applicant is a 43-year-old computer programmer for a Department of Defense contractor who seeks to maintain his security clearance. He has been employed in his current position since February 2006. He has held a security clearance since 2001. He has a bachelor's degree in computer science. He married on September 12, 2009. He is separated from his wife and is in the process of filing for divorce. He has no children. (Tr. 5-6; 23; Gov 1)

In June 2004, Applicant applied for access to sensitive compartmented information (SCI). In December 2004, he underwent a polygraph test. Applicant wanted to make sure that he passed the polygraph test. Before he took the test, he told the polygrapher there were a few items he needed to explain. He told her that between May 2002 and March 2003, he claimed more hours at work than he actually worked. On occasion, he would take a longer lunch than he was supposed to and sometimes left work early if all of his work was completed. He also indicated that he had viewed sexually explicit material on his work computer. Over a period of six to eight months, Applicant would receive unsolicited e-mails containing pornographic information. He was not aware the e-mails were pornographic until he opened them. He would immediately delete them. He realized that he should have reported the e-mails immediately. The unsolicited e-mails stopped appearing when his computer was cleaned for an unrelated reason. (Tr. 25-34; Gov 4; Gov 5)

In 2006, Applicant received a letter from another government agency denying his access to SCI. He believes his SCI access was denied for the reasons stated above. He did not save the letter and did not appeal the denial of SCI access. The letter informed Applicant that his security clearance was still valid for SECRET and below. He did not appeal because he can find work as a computer programmer elsewhere. (Tr. 15-16, 40-41, 45; Gov 2; Gov 4)

Applicant testified that he exaggerated the number of hours that he claimed for work that he did not work because he wanted to make sure that he passed the polygraph. He told the polygrapher that he overcharged 20 hours. He actually over-

charged between two and four hours a week. One of the reasons that he overcharged his employers for hours that he did not work was because he was angry that he did not get the job positions that he wanted. He has not overcharged his employers for hours that he did not work since this incident. (Tr. 34-40; Gov 2)

There is nothing in the record from the other government agency indicating the basis for denying his access to SCI in 2006. In fact, there is nothing in the record from the other government agency verifying that Applicant's access to SCI was denied in 2006.

Applicant worked for two-and-a-half years with access to SECRET information without incident. In December 2009, he accepted his current position for better opportunities. (Tr. 45) A performance evaluation covering the period December 1, 2008 to November 20, 2009, states that he meets or exceeds standards. (AE A)

A friend who has known him since 2000 wrote a letter indicating that Applicant is one of the most brilliant, helpful, honest, and generous individuals that she has ever met. She describes him as an "exceptionally honest individual with a lot of integrity." She trusts him and states he is the first to offer a helping hand to anyone who needs it. (AE B) Another friend has known him for ten years. He has never observed any behavior that he thought would disqualify him for a security clearance. He describes Applicant, "as an honest and sincere person of high character and strong professional integrity." (AE C)

Policies

When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the adjudicative guidelines. In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially disqualifying conditions and mitigating conditions, which are required 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.

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 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.

The following personal conduct disqualifying conditions potentially apply to the facts of this case:

> 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: (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; (2) disruptive, violent, or other inappropriate behavior in the workplace; (3) a pattern of dishonesty or rule violations; (4) evidence of significant misuse of Government or other employer's time or resources).

AG ¶¶ 16(d)(3) and 16(d)(4) apply because Applicant admits that between May 2002 and March 2003, he claimed that he worked more hours than he did at his former employers. He also admits to exaggerating the hours that he falsely claimed he worked to the polygrapher in hopes that he would pass the polygraph test. His conduct reveals a pattern of dishonesty and significant misuse of his employer's time and resources.

SOR ¶1.a is found for Applicant. While Applicant admits that from 2001 to 2002 he viewed pornographic e-mails on his work computer, he opened these e-mails inadvertently and immediately deleted them when he saw them. There is no evidence that he downloaded pornographic files to his work computer. Applicant was conscientious during his pre-polygraph interview when he disclosed this information. Based on the record evidence, Applicant's conduct alleged in SOR ¶ 1.a does not raise a security issue under personal conduct.

The following personal conduct mitigating condition applies to Applicant's case:

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).

AG ¶ 17(c) applies because the conduct which was the basis for denying SCI access for Applicant happened between May 2002 and March 2003, over seven years ago. It does not cast doubt on Applicant's present reliability, trustworthiness, or good judgment. If anything, Applicant appears to overcompensate in the honesty department. After his TS/SCI access was denied, Applicant still had access to SECRET information and handled SECRET documents without any security incidents. He no longer claims hours for work that he has not performed. The security concerns raised under personal conduct are mitigated.

Guideline M, Use of Information Technology Systems

The security concern relating to the guideline for Use of Information Technology Systems is set out in AG ¶ 39 which states,

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 hardware, software, firmware, and data used for the

> communication, transmission, processing, manipulation, storage, or protection of information.

Under Guideline M, disqualifying condition AG ¶ 40(e) (unauthorized use of a government or other information technology system) potentially applies in Applicant's case with respect to SOR ¶1.a. I find that it does not apply. Although Applicant admitted to opening e-mails that contained sexually explicit content on his work computer during work hours, additional clarification during the hearing revealed that Applicant inadvertently opened these e-mails and was unaware of the content. Once he discovered the content of the e-mails, he immediately deleted them. He did not actively seek out files containing sexually explicit material. While not privy to the basis of the other government agency's denial of Applicant's access to SCI in 2006, I found him to be credible during the hearing. The issue raised under the Use of Information Technology Systems concern 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) 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 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. While Applicant's explanation for the reason he was denied access to SCI was unusual, it was credible. There is nothing in the record which contradicts his testimony. He has not attempted to claim more hours than he actually worked since March 2003. He has learned a lesson. His performance evaluation and his reference letters support the premise that there is nothing in Appellant's behavior or character which would raise doubts about his current reliability, trustworthiness, and good judgment. The personal conduct concerns are mitigated. The Government did not meet its burden of proof to raise the Use of Information Technology concern.

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:	FOR APPLICANT
Subparagraphs 1.a-c:	For Applicant
Paragraph 2, Guideline M:	FOR APPLICANT
Subparagraph 2.a:	For Applicant

Conclusion

In light of all of the circumstances presented by the record in this case, it is clearly consistent with the national interest to grant Applicant eligibility for a security clearance. Eligibility for access to classified information is granted.

_____
ERIN C. HOGAN
Administrative Judge