DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 09-02392
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Melvin A. Howry, Esquire, Department Counsel

For Applicant: *Pro se*

May 17, 2010

Decision

O'BRIEN, Rita C., Administrative Judge*:*

Based on a review of the case file, pleadings, and exhibits, I conclude that Applicant has not mitigated the security concerns raised under the guidelines for use of information technology systems, handling protected information, and personal conduct. Accordingly, his request for a security clearance is denied.

Applicant submitted an Electronic Questionnaire for Investigations Processing, which he signed on August 28, 2008. 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 for a security clearance.

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

On August 24, 2009, DOHA issued to Applicant a Statement of Reasons (SOR) that specified the basis for its finding: security concerns addressed in the Directive under Guideline M (Use of Information Technology Systems), Guideline K (Handling Protected Information), and Guideline E (Personal Conduct) of the Adjudicative Guidelines (AG).[2] Applicant signed his notarized Answer September 14, 2009, in which he admitted all the allegations in the Statement of Reasons except the following: 1.a., 1.b., 2.b., 3.a., 3.b., 3.e., and 3.f. He also requested a decision without a hearing.

On November 16, 2009, DOHA Department Counsel submitted a file of relevant material (FORM) in support of the government's preliminary decision to deny Applicant's request to be granted a security clearance. The FORM contained eight documents, identified as Government Exhibits (GE) 1 through 8. The FORM and exhibits were forwarded to Applicant. He received the package on November 25, 2009, and submitted a Reply to the FORM. The case was assigned to another administrative judge, and subsequently transferred to me on March 5, 2010, for an administrative decision based on the record. Subsequently, Applicant submitted am additional document, signed on May 3, 2010. Department Counsel did not object, and I admitted the document to the record as Applicant Exhibit (AE) A.

Findings of Fact

Applicant's admissions to the SOR allegations are incorporated herein as findings of fact. After a thorough review of the pleadings and the record evidence, I make the following additional findings of fact.

Applicant is 60 years old. He has been married since 1974 and has two sons, 18 and 25 years of age. He earned a masters degree in 1992. Since 1980, he has worked for the same defense contractor, where his holds the position of principal systems administrator. (GE 4)

Applicant held a security clearance since 1981, at the secret and top secret levels. (GE 4) During the course of his security investigations, Applicant disclosed information about his conduct while he performed his job as a systems administrator from the 1990s to 2006. Based on findings from these investigations, his program access was revoked on September 18, 2006 by another government agency (AGA). He appealed the decision, and wrote a Response to the allegations ("Response"), dated November 1, 2006. (GE 7, p. 27-38) The decision to revoke was affirmed in August 2007. (GE 7, p. 22-23)

[2] Adjudication of this case is controlled by the Adjudicative Guidelines (AG), which apply to all adjudications or trustworthiness determinations in which an SOR was issued on or after September 1, 2006.

In performing his job as a systems administrator, Applicant worked on his coworkers' computers to repair problems or improve performance. Applicant looked at material he thought was classified on a co-worker's computer, without having a "need to know" the contents.[3] During a security interview on May 26, 2006, he admitted that he did not have a need to know the contents of the file, and looked at the document because he was curious. (GE 7, p. 70) However, in his November 2006 Response, he notes that he had to see the file contents in order to be sure that the file had been repaired. (GE 7, pp. 30-31) During the May 2006 interview, he also discussed looking at a document on his supervisor's computer in 1999. His supervisor at the time was the lead on a project at a branch office that Applicant's company was supporting. The material was classified, and Applicant did not have a need to know the information. He admitted that he sometimes looked at material on employees' computers because he was curious. (GE 7, pp. 9, 70-71) In his post-hearing submission of 2010, Applicant notes that he was recently informed by "the supervisor" (not further identified) that if he received permission to work on a computer, then he was considered to have a need to know the information he would see in the process of performing that work. Applicant stated he was unaware of this fact when he viewed classified material on other worker's computers in the past. (AE A)

Applicant also admitted, during a security interview on July 23, 2001, that he removed computer parts from company computers and used them in his home computer. The parts, including a small computer system interface (SCSI) card and floppy disks, were from unclassified computers. (GE 7, p. 78) In his Answer, Applicant denies this allegation, calling it a "total fabrication." (GE 3)

In about 2005–2006, Applicant used the classified passwords of four coworkers to access their accounts to work on email and start-up issues. (GE 7, p. 9, 60, 63) Applicant noted in his FORM Reply that the coworkers gave him their passwords and "I didn't argue with them."

In his May 2006 security interview, Applicant stated that in about 2001, his supervisor was not allowing him to do enough work on their team. He used his system administrator access to look at files on her personal drive to check if she was leaving him out of some of the work. He stated he looked only at file titles, not content. However, in his July 2001 interview, Applicant admitted opening two of his supervisor's computer files. In his February and April 2001 interviews, he stated he accessed his supervisor's files out of curiosity. (GE 7, p. 58, 72, 78)

During the May 2006 interview, Applicant was also asked if he had gone through his supervisor's desk. Applicant became emotional, cried, and stated he had not told any security officials of this "deep dark secret," but that in 2001 he had gone through her desk to find out her salary. However, in his Response of November 2006, Applicant

[3] The date of this event is unclear. SOR ¶ 2.a places it in the "late 1990s." Applicant noted in his interview of May 2006 that it occurred "one to two years ago," which would have been 2004 – 2005. (GE 7, p. 70) However, in his Answer of November 1, 2006, he said it occurred in 1995. (GE 7, p. 30)

stated that he had permission to go through her desk to look for diskettes, and that he saw the salary information inadvertently. (GE 7, pp.30, 72)

In the July 2001 security interview, Applicant admitted downloading pornographic material from the internet to a company computer every few months between 1998 and 2001, spending 45 to 60 minutes each time. The most recent occurrence (at that point in time) was in July 2001. (GE 7, p. 78) Applicant contends in his FORM Reply that he did not download pornographic material, but simply viewed it. He also questions whether the material he viewed, similar to photographs in adult magazines, is pornography.

In January 2002, Applicant's employer issued him a letter of reprimand that stated, in pertinent part,

> …while at work you were looking at pornographic images while you were involved with inappropriate personal conduct.[4] As a condition for working with sensitive, national security level program information, you are required, per U.S. Government policy, to maintain the highest standards of personal conduct. The above aspects of your behavior are, or have been in violation of this policy.

The letter concluded that future personal conduct incidents could lead to revocation of his access, and that his signature indicated his acknowledgement and understanding of the policy. On January 2, 2002, Applicant signed the letter. (GE 7, p. 106)

In 2006, Applicant violated security rules by carrying a flash memory device into a Sensitive Compartmented Information Facility (SCIF) between four and eight times. He stated he did not realize the device was in his pocket. (GE 3, GE 7, p. 9-10, 60) During his security interview of July 2006, he admitted that, in February 2006, he knowingly brought an activated cell phone into the SCIF. After checking that no one was in the SCIF, he entered it with his cell phone turned on. He knew it was prohibited by security rules, but did it for the thrill, and to see if he could avoid being caught. (GE 7, p. 60) In his November 2006 Response, Applicant stated that this was a "minor mistake in judgment" and that he will not do it again. (GE 7, p. 33) In 2006, Applicant also left a classified document unsecured for two to three days. Although it was inside the SCIF, it was not in a locked safe, as required. He was verbally reprimanded by his program security officer. (GE 7, p. 62, 71)

[4] The letter does not specify the nature of the "inappropriate personal conduct." However, during the July 2001 interview, Applicant admitted masturbating at work, approximately five times, once in February 2001, and at other times four to six years earlier. (GE 7, p. 76) However, in his May 2006 security interview, he denied masturbating at work. (GE 7, p. 63, 71) There is no indication whether the inappropriate conduct cited by Applicant's company's letter was masturbation. This conduct is not alleged, and will not be considered as part of the Whole-Person analysis because Applicant did not have notice that it was an issue in his case.

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 AG.[5] Decisions must also reflect consideration of the "whole person" factors listed in ¶ 2(a) of the Guidelines.

The presence or absence of disqualifying or mitigating conditions does not determine a conclusion for or against an applicant. However, specific applicable guidelines should be followed when a case can be so measured, as they represent policy guidance governing the grant or denial of access to classified information.

A security clearance decision is intended only to resolve the question of whether it is clearly consistent with the national interest[6] for an applicant to 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. Additionally, the government must be able to prove controverted facts alleged in the SOR. If the government meets its burden, it falls to applicants to refute, extenuate or mitigate the government's case. Because no one has a "right" to a security clearance, applicants bear a heavy burden of persuasion.[7] A person who has access to classified information enters a fiduciary relationship based on trust and confidence. The government has a compelling interest in ensuring that applicants possess the requisite judgment, reliability, and trustworthiness to protect the national interest 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 to classified information in favor of the government.[8]

Analysis

Guideline M, Use of Information Technology Systems

AG ¶ 39 expresses the security concern related to use of information technology systems:

---

[5] Directive. 6.3.

[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).

> 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.

AG ¶ 40 describes disqualifying conditions that could raise a security concern, including the following relevant conditions:

> (a) illegal or unauthorized entry into any information technology system or component thereof; and
>
> (e) unauthorized use of a government or other information technology system.

As a systems administrator, Applicant was able to access other workers' computer files. In 2001, he used his status to gain unauthorized entry into his supervisor's personal computer files. Also in 2001, Applicant engaged in unauthorized use of an information technology system when he viewed pornographic material on a company computer. Disqualifying conditions 40(a) and 40(e) apply.

AG ¶ 41 provides the following relevant mitigating conditions:

> (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;
>
> (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
>
> (c) the conduct was unintentional or inadvertent and was followed by a prompt, good-faith effort to correct the situation and by notification of a supervisor.

After using a company computer to view pornography in 2001, Applicant received a letter of reprimand and was warned that such conduct in the future would place his access in jeopardy. Applicant also used his system administrator access to satisfy his personal desire to see sensitive information in his supervisor's personal computer files. His actions occurred during his routine work, not in unusual circumstances. Moreover,

his conduct was neither minor nor inadvertent; he committed serious and intentional breaches of the trust placed in system administrators. Although this conduct occurred several years ago, the intentional nature of Applicant's actions, and the gravity of his breach of trust outweigh the distance in time. AG ¶ 41(a), (b), and (c) do not apply.

Guideline K, Handling Protected Information

AG ¶ 33 expresses the security concern pertaining to handling protected information:

> 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.

The following disqualifying conditions under AG ¶ 34 raise a security concern:

> (f) viewing or downloading information from a secure system when the information is beyond the individual's need-to-know;
>
> (g) any failure to comply with rules for the protection of classified or other sensitive information; and
>
> (h) negligence or lax security habits that persist despite counseling by management.

Applicant violated security rules numerous times in 2006. He admits bringing a flash memory device into the SCIF, claiming it was inadvertent. However, Applicant brought the device in not once or twice, but four to eight times. During the same time period, he carried an activated cell phone into the SCIF. Applicant admitted to a security investigator that he brought the cell phone into the SCIF intentionally, for the thrill, and to see if he could "get away with it." He also failed to secure a classified document within the SCIF. These events all occurred within the short time frame in 2006 before his access was suspended in March 2006. AG ¶ 34 (g) applies to Applicant's deliberate failure to follow security rules about the flash device and the cell phone. I find that AG ¶ 34(h) applies to his negligent conduct in failing to secure a classified document,. However, it applies only in part, because the record does not indicate if Applicant was counseled.

Applicant also admitted during security interviews that he viewed material on co-workers' classified computers because he was curious, although he did not have a "need to know" the information. In 2001, he specifically sought to and did access sensitive information in his supervisor's computer files that he was not authorized to view. He also viewed a document in 1999 on the computer of another supervisor at a branch office. AG ¶ 34(f) applies.

AG ¶ 35 provides conditions that could mitigate security concerns, including the following relevant condition:

> (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.

Applicant's actions did not occur under unusual circumstances, but rather in the regular course of his duties. Although several occurred approximately ten years ago, some events happened in 2006, about four years ago, which is more recent. Applicant committed a series of security violations in 2006, all before his access was suspended in March 2006. The record contains no indication of further security violations, but this may stem from the fact that Applicant's access was revoked in September 2006. Adherence to security rules is key to the industrial security program. Applicant's actions reflect poorly on his reliability and trustworthiness, and AG ¶ 35(a) does not apply.

Guideline E, Personal Conduct

> AG ¶ 15 expresses the security concern pertaining to personal conduct:
>
> 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.

AG ¶ 16 describes conditions that could raise a security concern and may be disqualifying. The following conditions are relevant:

> (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;…

> (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…;

The SOR alleges that in 2001, Applicant deliberately searched his supervisor's desk for salary information. In November 2006, Applicant denied this allegation. However, a few months earlier, during a security interview in May 2006, Applicant admitted doing so. I find that he did not view his supervisor's salary information inadvertently, and his claim that it was unintentional is misleading and an attempt to avoid responsibility for his conduct. Moreover, when he admitted going through her desk, he cried, and called his actions a "deep, dark secret" that he had not disclosed to any security officials. His behavior and statements indicate that his conduct was embarrassing to him, and that he wished it to remain secret. AG ¶ 16(e) applies. In addition, although Applicant vehemently denied this SOR allegation, the evidence shows he admitted in July 2001 that he removed company computer parts for use in his personal computer. His conduct was untrustworthy behavior that falls under AG ¶ 16(d)(1).

AG ¶ 17 provides conditions that could mitigate security concerns under Personal Conduct guideline. The following conditions are relevant:

> (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;
>
> (e) the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress;

AG ¶ 17(c) does not apply, for the reasons discussed under Guidelines M and K. Regarding mitigating condition AG ¶ 17(e), Applicant's behavior when he disclosed that he looked in his supervisor's desk shows that he was very embarrassed by it, and he admitted that he had not disclosed it to his security officer. It constitutes a basis for exploitation. As the record evidence does not show when or if Applicant ever disclosed his conduct to his supervisor, security officer, or anyone else, there is no way to discern if it still represents a source of vulnerability to exploitation. Under the Appeal Board's jurisprudence, however, even if it has now been disclosed, Applicant was vulnerable to exploitation during the period when it had not been disclosed and remained a secret.[9] AG ¶ 17(e) does not apply.

[9] ISCR Case No. 91-0259 at 5 (App. Bd. Oct 7, 1992).

Whole-Person Analysis

Under the whole-person concept, an administrative judge must evaluate the Applicant's security eligibility by considering the totality of the Applicant's conduct and all the relevant 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.

AG ¶ 2(c) requires that the ultimate determination of whether to grant a security clearance be an overall commonsense judgment based upon careful consideration of the guidelines and the whole-person concept. Under the cited guidelines, I considered the potentially disqualifying and mitigating conditions in light of all the facts and circumstances surrounding this case.

Applicant looked at coworkers' classified files, deliberately viewed his supervisor's personal computer files and private information in her desk, and obtained workers' classified passwords while he worked on their computers. He made himself vulnerable to exploitation because he engaged in conduct that was embarrassing and that he did not want revealed. He entered a SCIF with prohibited items, including an active cell phone and a flash device. He failed to secure a classified document and was reprimanded. He viewed pornography at work, and his company issued him a letter of reprimand. His conduct cannot be mitigated based on youthful indiscretion, because he was a mature adult between 45 and 55 years of age when these events occurred. Each time he knowingly engaged in this conduct, he placed his own desires above the government's need for reliable and trustworthy conduct in those to whom it grants security clearances.

Although much of the conduct in the SOR is old, the repeated nature of Applicant's untrustworthy actions, from the 1990s to 2006, is a concern. Moreover, a person who violates rules, particularly when it is intentional, undermines the trust that is key to the success of the security program. There is no evidence in the record of problems between 2002 when Applicant received the letter of reprimand, and 2006. But at that point, Applicant had numerous security lapses, and also deliberately violated security rules for the thrill of it. This re-emergence of security violations raises concerns. In addition, he has given incomplete and conflicting information during his numerous security interviews and responses to the government. The fact that Applicant engaged in untrustworthy conduct while held a security clearance is most significant,

and raises doubts about whether he is willing or able to avoid recurrence of such behavior in the future and to fulfill the obligations imposed on those who are granted security clearances.

Overall, the record evidence fails to satisfy the doubts raised about Applicant's suitability for a security clearance. For all these reasons, I conclude Applicant has not mitigated the security concerns arising from the cited adjudicative guideline.

Formal Findings

Paragraph 1, Guideline M	AGAINST Applicant
Subparagraphs 1.a. - 1.c.	Against Applicant
Paragraph 2, Guideline K	AGAINST Applicant
Subparagraphs 2.a. - 2.f.	Against Applicant
Paragraph 3, Guideline E	AGAINST Applicant
Subparagraphs 3.a. - 3.f.	Against Applicant

Conclusion

In light of all of the circumstances presented by the record in this case, it is not clearly consistent with the interests of national security to allow Applicant access to classified information. Applicant's request for a security clearance is denied.

RITA C. O'BRIEN
Administrative Judge