DATE: June 28, 2004

In Re:

SSN: ----------

Applicant for Security Clearance

CR Case No. 02-17219

DECISION OF ADMINISTRATIVE JUDGE

MATTHEW E. MALONE

APPEARANCES

FOR GOVERNMENT

Eric H. Borgstrom, Esquire

Department Counsel

FOR APPLICANT

Dennis J. Sysko, Esquire

SYNOPSIS

Applicant committed six security violations between 1996 and 2001. Four violations occurred while employed by one defense contractor between 1996 and 1998, the other two while at another job. Applicant's claims his violations were caused in part by recently diagnosed attention deficit disorder (ADD) and by other external factors do not mitigate the security concerns engendered by his conduct. Nor has he presented sufficient evidence of mitigation through rehabilitation. While he has mitigated the Guideline M security concerns, Applicant is disqualified under Guideline K and for related Guideline E concerns. Clearance is denied.

STATEMENT OF THE CASE

On July 22, 2003 the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) to Applicant. The SOR informed Applicant that DOHA adjudicators could not make a preliminary affirmative finding that it is clearly consistent with the national interest to continue Applicant's security clearance.[(1)] The SOR alleges facts which raise security concerns under Guideline E (Personal Conduct), Guideline K (Security Violations), and Guideline M (Misuse of Information Technology Systems).

On November 12, 2003, Applicant executed a notarized response to the SOR wherein he admitted with explanation all of the SOR allegations and requested a hearing.[(2)] The case was assigned to me on March 22, 2004. DOHA issued a Notice of Hearing setting this case to be heard on April 16, 2004. All parties appeared as scheduled, submitted exhibits [(3)] and witness testimony in support of their respective cases, and DOHA received the transcript (Tr) on April 29, 2004.

FINDINGS OF FACT

After a thorough review of the pleadings, transcript, and exhibits, I make the following essential findings of fact:

Applicant is a 45-year-old employee of a defense contractor. He seeks a clearance in connection with his duties as an engineer on his company's contract with the Department of Defense. He has been married to the same woman for 15 years and is the father of two young children. He has held a security clearance continuously since 1991.

Applicant received a bachelor's degree in electrical engineering from his state's major public university in 1981 and went to work the next month as a senior engineer at company A. In January 1983, while still working full time, he began working toward his masters in electrical engineering at his state's best private university. He received his masters degree in 1988 and continued what appears to have been a successful tenure at company A.

In the early to mid-1990s, company A experienced a series of lay-offs causing Applicant to look for employment options elsewhere. He went to work for company B in February 1996 as a senior staff member. Applicant soon became aware of a very different corporate culture at company B. Procedures such as time keeping and security accountability were apparently more closely regulated than at company A, where a more casual atmosphere prevailed. By his own admission, Applicant found himself doing a job for which, at times, he may have been under-qualified. He worked at company B until October 1998, but he has characterized his tenure there as generally unpleasant.

On December 2, 1996, Applicant was assigned to perform "end-of-day" checks for the office space where he and his co-workers were located. This entailed checking for unlocked safes, improperly secured computers, classified documents left unsecured, etc. These duties rotated among employees at company B on a weekly basis. When Applicant's week came up, he was absent from work the first two days to attend to personal matters - he and his wife were closing on and moving into a new house. Applicant also had a final exam in a business math course he was taking at the local community college. When Applicant went to work on Wednesday of that week, he forgot about his end-of-day duties. He was counseled for his omission, and it was determined there was little or no risk of compromise of classified information as a result.

On June 19, 1997, Applicant attempted to create an unclassified automated document using unclassified information from an otherwise classified automated document. His intent was to generate a file he could give to other members of a project team he was on so all would know what the statement of expected work was. He unintentionally included in his new document a classified radio frequency. Applicant's supervisor discovered this violation when he saw a printed version of Applicant's new file. To further compound this violation, in creating his new document Applicant had put classified information on a computer system rated only for unclassified data. Again, Applicant was counseled about the need to adhere to established rules for safeguarding classified information. He was also issued an official reprimand for his actions and advised of the requirements in the National Industrial Security Program Operating Manual (NISPOM) for safeguarding classified information.[(4)]

On August 4, 1997, Applicant signed out two classified documents from the classified storage container in his group's office. The person from whom he received the documents advised Applicant they were classified. Applicant used the documents in his work that day and left them both on his desk when he went home that evening. On August 5, Applicant continued to use both documents but returned one to the storage container later that day. The other document was again left on Applicant's desk when he left for the day. A company security guard making his rounds later that evening confiscated the document and returned it to proper storage. It was eventually determined that no compromise of classified information had occurred because Applicant had locked his office door when he left and the only other persons who accessed the space were staff members with the proper clearance. Applicant's version of these events omits any mention of a second document. He also explained his violation by stating that the color scheme of the document made it difficult to see the classified markings. He also denied any knowledge of a "logging in process" for classified documents.[(5)]

On July 8, 1998, Applicant was cited for another security violation. While working on a classified automated spreadsheet containing information about surface-to-surface missile threats sorted by the countries possessing those missiles, Applicant attempted to generate an unclassified spreadsheet substituting integers for country names to avoid linking a country with a known missile system. In so doing, Applicant inadvertently left a legend showing each integer and the country it corresponded to in the new spreadsheet. Again, this security violation also included improper storage of classified data on an unclassified computer. However, in this instance, he physically transferred the classified file

from one system to another using a diskette. Management subsequently confiscated Applicant's computer and found two other files in his hard drive he had created in the preceding months using the same software program. His superiors took corrective measures to delete the files and to monitor Applicant's actions in using his computer and handling classified information generally. Applicant was reprimanded and suspended without pay for one week following the July 1998 incident.[(6)] In neither this instance nor with respect to his actions in June 1997 was Applicant authorized to decide which information in the original files was classified and which was unclassified.[(7)]

Soon thereafter, Applicant left company B and briefly worked for company C. However, the commute to company C was lengthy and after about nine months, he left to take a position with company D closer to home. His tenure at company C was very pleasant and he would have stayed were it not for the time commuting and its impact on his time at home to help his wife with their two young children. Applicant started at company D in June 1999 and stayed there until accepting his current position at company E in June 2003.

At company D, Appellant shared an office with another engineer. Each had his own classified computer, the hard drive for which was to be removed at when unattended and placed in a safe. This is by design an easy procedure so as to facilitate proper storage of classified material on the hard drive without taking too much time or effort. On December 1999, while working for company D, Applicant agreed to watch his office mate's classified computer while the office mate stepped out for a few minutes. As it turned, Applicant's office mate was gone for almost three hours. The screen saver was active making the computer screen blank so it was not apparent the machine was still on. and Applicant forgot it was still running when he left for the day. After he left, a company security officer doing end of the day checks discovered the classified computer unattended with the hard drive still installed. When this discrepancy was investigated, Applicant readily volunteered he had left the machine unattended. No report of this incident was ever made and he was informally counseled concerning the importance of properly adhering to procedures.

On April 10, 2001, Applicant left a classified document on his desk over night. The document was discovered during an after-hours check by security. He explained that the document was covered by other documents on his desk and he simply did not see it when he left for the day. He was reprimanded and counseled for this violation.

Applicant and his wife have two children. The younger child was born in March 1997 and suffered from a series of ear infections and what was eventually diagnosed as acid reflux disease. The pain from these two conditions caused the baby to sleep only in 40-minute increments for the first 18 months. It was not until about October 1998 that the child's condition abated through medical treatment and natural development of his digestive system. As might be expected, Applicant and his wife did not sleep very well and were under a great deal of stress during that time. However, Applicant continued to go to work and school, fulfilling his responsibilities there and at home.

In January 2004, Applicant began seeing a psychologist who has diagnosed him as having attention deficit disorder (ADD). Applicant has been prescribed medication for this condition and has apparently benefitted from it as he is more productive at work and has more energy in general. This view is shared by his wife and some co-workers.[(8)] He currently works for a small business with a sub-contractor relationship to a large, nationally-known defense contractor. The large, primary contractor is responsible for document management and other safeguards such as end-of-day checks. The president (who also serves as facilities security officer) of Applicant's current company has offered a rehabilitative strategy outlining steps the company will take to help ensure Applicant does not commit further security violations.[(9)]

POLICIES

The Directive sets forth adjudicative guidelines[(10)] to be considered in evaluating an Applicant's suitability for access to classified information. The Administrative Judge must take into account both disqualifying and mitigating conditions under each adjudicative issue applicable to the facts and circumstances of each case. Each decision must also reflect a fair and impartial common sense consideration of the factors listed in Section 6.3 of the Directive. 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. Having considered the record evidence as a whole, I conclude the relevant adjudicative guidelines to be applied here are Guideline E (Personal

Conduct), Guideline K (Security Violations), and Guideline M (Misuse of Information Technology Systems).

BURDEN OF PROOF

A security clearance decision is intended to resolve whether it is clearly consistent with the national interest[(11)] for an Applicant to either receive or continue to have access to classified information. The Government bears the initial burden of proving, by something less than a preponderance of the evidence, controverted facts alleged in the SOR. If the government meets its burden it establishes a *prima facie* case that it is not clearly consistent with the national interest for the Applicant to have access to classified information. The burden then shifts to the Applicant to refute, extenuate or mitigate the Government's case. Because no one has a "right" to a security clearance, the Applicant bears a heavy burden of persuasion.[(12)] 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.[(13)]

CONCLUSIONS

Guideline M (Misuse of Information Technology Systems). Under this guideline, a security concern exists where it is shown an applicant has failed to comply with rules, procedures, guidelines or regulations pertaining to information technology systems. Such conduct raises questions about an individual's trustworthiness, willingness, and ability to properly protect classified systems, networks, and information. The term "Information Technology Systems" includes all related equipment used for the communication, transmission, processing, manipulation, and storage of classified or sensitive information.[(14)] Department Counsel has established a *prima facie* case for disqualification under this guideline. Applicant twice improperly stored classified information in a computer authorized to contain only unclassified information. On the second occasion (SOR 1.d), Applicant used a diskette to transfer a classified file to an unclassified system. Of the listed disqualifying conditions (DC), I conclude only DC 4[(15)] applies. The diskette he used constitutes media within the plain meaning of DC 4. Although Department Counsel has not cited to a specific rule, procedure or guideline specifically prohibiting Applicant from acting as he did, I conclude on the strength of his earlier violation and reprimand (SOR 1.b) he knew or should have known he was not allowed to move classified information to an unclassified system.

Of the listed mitigating conditions (MC), only MC 1[(16)] applies. His misuse of information systems took place over six years ago, and there is no indication he has committed similar missteps since then. I have not applied MC 2[(17)] because Applicant's actions included a conscious decision to alter what he knew to be classified information and remove from the protection of the classified information system. MC 3[(18)] does not apply because Applicant was not authorized to put a classified diskette into an unclassified computer. Further, his July 1998 violation might be considered an isolated event as contemplated under this guideline because he did not use a diskette in the earlier violation; however, when company security officials inspected his computer after the second violation, they found two other classified files apparently transferred in the same way. Therefore, I conclude there is no mitigation available through MC 4.[(19)] MC 5 [(20)] does not apply because it was Applicant's managers and his company's security staff and not Applicant who took corrective action. The requirement under MC 5 for "prompt, good faith" action places the onus on Applicant to recognize what happened and take corrective measures as soon as possible, even if those measures might be adverse to Applicant's own interests.

The absence of similar conduct since 1998, even though he still uses classified information technology systems on a daily basis, sufficiently mitigates the government's concerns. On balance, I conclude in favor of Applicant with respect to Guideline M.

Guideline K (Security Violations). Under this guideline, a security concern exists when it is shown a person does not comply with security regulations. Such conduct raises doubt about an individual's trustworthiness, willingness, and ability to safeguard classified information. Department Counsel has established a *prima facie* case for disqualification

under this guideline. Applicant neglected his assigned duties when he failed to perform an end-of-day check of his staff's work area. (SOR 1.a) By itself, this would have been a minor infraction with little or no significance relative to Applicant's suitability for clearance. However, six months later he inadvertently included classified information in an unclassified file. (SOR 1.b). He was reprimanded and counseled about the need to be more careful when examining the information he was using. Two months later, Applicant was suspended without pay for leaving a classified document on his desk overnight when it should have been returned to proper storage. (SOR 1.c) Applicant's version of this event conflicts with the company security staff report in that the latter shows he knew the document was classified and had left the document unprotected for two nights not one. I do not accept Applicant's explanation that his violation stemmed from his inability to discern the classified markings on the document. The following summer, Applicant committed a fourth violation when he transferred a classified file to an unclassified computer. (SOR 1.d) He was suspended for a week without pay for this infraction. For the same reasons discussed under Guideline M, above, I conclude this violation was neither unintentional nor inadvertent.

Applicant's first four violations occurred during his tenure with company B. Applicant asserts they were due in part to the stress of his difficulties at home, to what has since been diagnosed as ADD, and to the work atmosphere at company B, which he describes as more tense and demanding than at his other jobs. However, Applicant continued to commit violations after he left company B and after the 18 months of difficulty with his child's acid reflux condition. He committed violations at company D in 1999 and 2001, but has not asserted he had any problems with the work atmosphere there or that the stressors of his home life played any part of these violations.

I do not accept Applicant's claim that, because he suffers from ADD, this condition, in hindsight, contributed to his security violations. The violation cited in SOR 1.b involved a deliberate decision by Applicant to transfer information, regardless if he knew it was classified. After he was counseled and reprimanded he essentially repeated the act through his conduct alleged in SOR 1.d. Further, his actions alleged in SOR 1.c reflect simple carelessness in handling classified documents and his explanation suggests he has been less than forthright about taking responsibility for his actions. If Applicant suffered from ADD when he committed his violations, he probably also suffered from it when he went to graduate school and when he was otherwise performing well at company A and tending to his obligations at home. I am also skeptical of his claims as he did not seek a diagnosis until after he had answered the SOR. If ADD could interfere with his ability to comply with simple procedures for safeguarding classified information, it would also have been a problem in other aspects of his life (something of which there is no record) and would probably have been addressed much earlier.

Applicant's actions constitute violations of specific requirements of the NISPOM. All of the violations are addressed by NISPOM section 5-100, a general requirement that all contractors and individual employees are responsible for safeguarding classified information in their custody. More specifically, SOR 1.a is addressed by NISPOM section 5-102; SOR 1.b and 1.d are addressed by NISPOM section 8-100, a general requirement aimed directly at classified automated information protection. Applicant's counsel has argued that Applicant's errors do not equate to the NISPOM definition of a security violation as contained in Appendix C. Counsel submits that Applicant only violated internal company procedures and not the requirements set forth in the NISPOM. I disagree. His employers, if they do business with the Department of Defense and use classified information, must implement internal procedures whereby they comply with the requirements of the NISPOM. If Applicant has failed to comply with, for example, his company's end-of-day procedures, he has failed to comply with a specific section of the NISPOM.

Of the listed Guideline K disqualifiers, DC 1[(21)] does not apply because there is no indication Applicant's actions resulted in actual disclosure of classified information. However, DC 2[(22)] applies due to Applicant's multiple violations, some deliberate and some owing to negligence. By contrast, Applicant's first violation in 1996 (SOR 1.a) and his violation in 1999 (SOR 1.e) were almost surely inadvertent. Given the busy personal schedule he had the week he forgot to do his end-of-day rounds, his error is understandable. Likewise, when he left his co-worker's computer unattended after several hours had passed and his co-worker's screen saver had blanked the screen. However, because he had been counseled after his other violations, which he argues were also inadvertent, I am unwilling to apply MC 1[(23)] to more than his first violation. Applicant's claims to mitigation are also undermined by the inconsistencies in his explanation about his August 1997 violation (SOR 1.c), the fact he was counseled, reprimanded, re-briefed and trained several times in response to his violations yet continued to commit security violations, and by the overall tenor of his defense; namely,

that there was an explanation or cause for his violations other than his own negligence or poor judgment.

MC 2[(24)] does not apply because Applicant committed multiple violations while employed at two different companies. Nor do I believe Applicant's violations were due to inadequate training. None of what he did could have been prevented by more training. They were errors of carelessness and of poor judgment. The fact they continued despite repeated counseling also precludes application of MC 3.[(25)]

The absence of any violations since 2001 benefits Applicant in assessing his suitability for clearance, and he has presented an earnest account of measures he now routinely takes to ensure he does not commit further violations. However, the corrective measures stated in his Answer amount to little more than what is normally expected of anyone with a clearance. Also, his current employer's willingness to monitor Applicant's procedural compliance and to enact other rehabilitative strategies contradicts a basic tenet of the personnel security program; that is, the government must be able to trust an individual to act responsibly at all times in safeguarding classified information and to adhere to rules and procedures intended for that purpose. The government should not have to rely on extra measures or conditions of access to ensure compliance with its rules for safeguarding classified information.

This is not to say that Applicant has not at least demonstrated a positive attitude toward his responsibilities in this regard, and I conclude MC 4 [(26)] applies here. However, the government must protect its sensitive interests by making predictive judgments based on past conduct, not on statements of what a person or his employer is willing to do. I conclude Guideline K against the Applicant.

Guideline E (Personal Conduct). Under this guideline, conduct involving questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations could indicate that the person may not properly safeguard classified information.[(27)] Of note in this case is the government's concerns about Applicant's judgment and reliability. The government has established a *prima facie* case for disqualification by showing the Applicant's security violations demonstrate unreliability regarding his duties to protect classified information. The government's case further shows Applicant has a history of disregarding rules and procedures for safeguarding classified information. Aside from the general Guideline E security concern noted above, DC 5[(28)] applies here. His violations are specifically addressed by sections of the NISPOM and Applicant signed agreements acknowledging his duty to protect classified information and to abide by rules and procedures in support thereof. Of the listed mitigating conditions, none apply here either because they are not relevant or because the facts do not support their application. I conclude Guideline E against the Applicant.

I have carefully weighed all of the evidence in this case, and I have applied the aforementioned disqualifying and mitigating conditions as listed under each applicable adjudicative guideline. I have also considered the whole person concept as contemplated by the Directive in Section 6.3, and as called for by a fair and commonsense assessment of the record before me as required by Directive Section E2.2.3. I conclude the evidence as a whole presents an unacceptable risk to the government's compelling interest in ensuring its classified information is properly safeguarded. I conclude that Applicant's access to classified information should not be continued at this time.

FORMAL FINDINGS

Formal findings regarding each SOR allegation as required by Directive Section E3.1.25 are as follows:

Paragraph 1, Guideline K: AGAINST THE APPLICANT

Subparagraph 1.a: For the Applicant

Subparagraph 1.b: Against the Applicant

Subparagraph 1.c: Against the Applicant

Subparagraph 1.d: Against the Applicant

Subparagraph 1.e: Against the Applicant

Subparagraph 1.f: Against the Applicant

Paragraph 2, Guideline M FOR THE APPLICANT

Subparagraph 2.a: For the Applicant

Subparagraph 2.b: Against the Applicant

Paragraph 3, Guideline E: AGAINST THE APPLICANT

Subparagraph 3.a Against the Applicant

DECISION

In light of all the circumstances presented by the record in this case, it is not clearly consistent with the national interest to grant or continue a security clearance for the Applicant.

Matthew E. Malone

Administrative Judge

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

2. Included with Applicant's Answer was a letter from his current Facility Security Officer (FSO) attesting to Applicant's suitability for a security clearance and value to the company's contract with DoD. There being no objection from Department Counsel, I have included it in the record as part of the Answer.

3. Government's Exhibits (GE) 1 through 16, and Applicant's Exhibits (AE) A through H. GE 15 is included in the record pursuant to Department Counsel's request I take administrative notice of its contents. GE 16 is included in the record for rebuttal purposes. AE 1 was admitted over objections of Department Counsel, subject to limitations as to how much weight could be assigned to it. (Tr., p. 52 - 53).

4. GE 2; Tr., p. 70 - 76, 80.

5. GE 2; GE 5; Tr., p. 78 - 81.

6. GE 2; GE 6; GE 7; GE 8.

7. Tr., p. 123.

8. Tr., p. 185 - 186; AE A; AE B.

9. Attachment to Answer.

10. Directive, Enclosure 2.

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

12. *See Egan,* 484 U.S. at 528, 531.

13. *See Egan;* Directive E2.2.2.

14. Directive, E2.A13.1.1.

15. Directive, E2.A13.1.2.4. Introduction of hardware, software or media into any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations;

16. Directive, E2.A13.1.3.1. The misuse was not recent or significant;

17. Directive, E2.A13.1.3.2. The conduct was unintentional or inadvertent;

18. Directive, E2.A13.1.3.3. The introduction or removal of media was authorized;

19. Directive, E2.A13.1.3.4. The misuse was an isolated event;

20. Directive, E2.A13.1.3.5. The misuse was followed by a prompt, good faith effort to correct the situation.

21. Directive, E2.A11.1.2.1. Unauthorized disclosure of classified information;

22. Directive, E2.A11.1.2.2. Violations that are deliberate or multiple or due to negligence.

23. Directive, E2.A11.1.3.1. [Violations] [w]ere inadvertent;

24. Directive, E2.A11.1.3.2. Were isolated or infrequent;

25. Directive, E2.A11.1.3.3. Were due to improper or inadequate training;

26. Directive, E2.A11.1.3.4 Demonstrate a positive attitude towards the discharge of security responsibilities.

27. Directive, E2.A5.1.1.

28. Directive, E2.A5.1.2.5. A pattern of dishonesty or rule violations, including violation of any written or recorded agreement made between the individual and the agency;