DATE: March 27, 2007

In re:

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

Applicant for Security Clearance

ISCR Case No. 03-05980

ISION OF ADMINISTRATIVE JUDGE

JUAN J. RIVERA

APPEARANCES

FOR GOVERNMENT

Candace Le'i, Esq., Department Counsel

FOR APPLICANT

Pro Se

SYNOPSIS

While employed by a defense contractor in 2000, Applicant accessed a classified network and copied and removed classified information from its location. He then transferred the information into his laptop computer, downloaded the information into an unclassified network, and shared the information with a co-worker. Applicant failed to present sufficient evidence to mitigate security concerns raised by his security violations and personal conduct. Clearance is denied.

STATEMENT OF THE CASE

On February 17, 2005, the Defense Office of Hearings and Appeals (DOHA) issued Applicant a Statement of Reasons (SOR) alleging facts that raise security concerns under Guideline K (Security Violations) and Guideline E (Personal Conduct). The SOR informed Applicant that, based on information available to the government, DOHA adjudicators could not make a preliminary affirmative finding that it is clearly consistent with the national interest to grant him access to classified information.[(1)] On March 22, 2005, Applicant answered the SOR (Answer),[(2)] and requested a clearance decision based on the written record without a hearing.

Department Counsel prepared a File of Relevant Material (FORM) which was mailed to Applicant on December 20, 2006. He acknowledged receipt of the FORM on January 16, 2007. Applicant answered the FORM on February 16, 2007, did not object to anything contained in the FORM, and submitted additional information for the administrative judge's consideration. The government did not object to Applicant's submission. The case was assigned to me on February 28, 2007.

FINDINGS OF FACT

Applicant admitted the SOR allegations in ¶¶1.a(1) - 1.a(4) with explanations. He denied the SOR allegations in ¶1.a(5) and ¶2.a. His admissions to the SOR allegations are incorporated herein as findings of fact. After a thorough review of

the FORM evidence and Applicant's submissions, I make the following additional findings of fact:

Applicant is a 42-year-old systems engineer with a highly distinguished career.[(3)] He married his wife in March 1989, and they have two daughters, ages nine and 13.[(4)] Applicant completed his master's degree in May 1991. From 1991 to 1992, he worked for a federal government agency. Between October 1992 and February 2003, he worked for a defense contractor, and through his outstanding performance of duty achieved the position of project engineer. In February 2003, Applicant's employment was terminated because his access to classified information was revoked as a result of the security violations which are the basis of the pending SOR.

In April 2003, Applicant and a colleague established their own consulting company. He seeks access to classified information to qualify for government contracts related to his area of expertise. Applicant also has worked as an adjunct instructor at a recognized university since June 2003.

Applicant was granted access to classified information at the secret level in December 1992, and to sensitive compartmented information (SCI) in March 1995. His employer provided him with education and training in the handling of classified information.[(5)] In April 2000, while working for a defense contractor, Applicant initiated a classified session on the network of a government agency.[(6)] He accessed a database which contained information with different classification levels. However, the different classification markings were not indicated. Applicant wrote down information from the database into in his daily planner and removed it from its classified location. Applicant averred he believed the information he removed was not classified because: some information was marked as unclassified, other was common knowledge, and other information was of no use without association with additional information.

Applicant was authorized to access the data, and his motives for accessing the information were apparently well intended. He wanted to be prepared to provide quick and accurate services to his government customers. Applicant copied and removed the classified information for his and his company's convenience. He needed the information to conduct rapid referencing of the data at remote working locations. His access to the classified facility was limited to working hours. Having the information with him avoided repeated visits to the classified facility. His project site office was small and had limited capability to handle classified information.[(7)] Applicant removed the information from its classified environment because he "(I) believed it to be unclassified and because of the need for its use at remote locations."[(8)]

Shortly after removing the information, Applicant discussed the data and his rationale for determining the information was not classified with his company manager. Although they could not reference to any specific declassification document, Applicant and his manager, on their own analysis determined that no unclassified or classified information was revealed through the data Applicant removed.

From April 2000 to January 2002, Applicant kept the information in his daily planner to use while working in government tasking when away from his desk. He made copies of the information for an office file and for a co-worker. He also copied the classified data into his laptop computer and downloaded the data into his company's unclassified network.[(9)] In 2001, Applicant attended two trade conferences in foreign countries, related to his area of expertise and the data he removed. He carried the classified information with him in his daily planer.[(10)]

In late 2002, Applicant was pending a polygraph interview as part of a routine periodic security investigation. While thinking about "unanswered security questions that could cause him any unease during the interview," he recalled the information he had taken from the classified network. He explained that, based on knowledge learned since removing the data, he realized the information he believed to be unclassified was, in fact, possibly classified.[(11)] In January 2002, Applicant asked one of his contacts (a military officer) whether the information was classified. He was told the information was classified at the secret level. Upon returning to his office, Applicant collected all copies of the information and placed them in a secure area. He then notified his security officer of the security violation. The ensuing security investigation determined that the information Applicant removed from the government's network was indeed classified. At the time he removed the data, Applicant did not have access to the document that showed the data was classified.

In 2002, Applicant's access to any DOD classified activity was suspended, and ultimately revoked because of his mishandling of classified information (i.e., the security violations which are the basis for the pending SOR). There is no evidence Applicant has ever been involved in any other security violations. He considers himself a security conscious individual and vehemently has stated he believed the information was not classified at the time he removed it. Because of this experience, he has learned a great deal about how to properly protect classified information.

Applicant's evidence convincingly establishes he is a hard-working and conscientious employee with impressive knowledge and capabilities. His performance appraisals show he is a topnotch engineer with an excellent history of accomplishments. He developed cutting edge capabilities that assisted his company and the government in projects of utmost importance. Those who know him best consider him a family man with the highest work ethic and morals. Furthermore, his appraisals and character reference letters established he was consistently rated satisfactorily for following his company's security policies, practices, and procedures.[(12)]

POLICIES

The Directive sets forth adjudicative guidelines which must be considered in evaluating an Applicant's eligibility for access to classified information. Foremost are the Disqualifying and Mitigating conditions under each adjudicative guideline applicable to the facts and circumstances of the case. However, the guidelines are not viewed as inflexible ironclad rules of law. The presence or absence of a disqualifying or mitigating condition is not determinative of a conclusion for or against an Applicant. Each decision must also reflect a fair and impartial common sense consideration of the factors listed in Section 6.3 of the Directive,[(13)] and the whole person concept.[(14)] Having considered the record evidence as a whole, I conclude Guideline K (Security Violations) and Guideline E (Personal Conduct) are the applicable relevant adjudicative guidelines.

BURDEN OF PROOF

The purpose of a security clearance decision is to resolve whether it is clearly consistent with the national interest to grant or continue an applicant's eligibility for access to classified information.[(15)] The government has the initial burden of proving controverted facts alleged in the SOR. To meet its burden, the government must establish a prima facie case by substantial evidence.[(16)] The responsibility 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 carries the burden of persuasion.[(17)]

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 to ensure 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 to classified information in favor of protecting national security.[(18)]

The decision to deny an individual a security clearance is not necessarily a determination as to the loyalty of the applicant.[(19)] It is merely an indication the applicant has not met the strict guidelines the President and the Secretary of Defense have established for issuing a clearance.

CONCLUSIONS

Under Guideline K (security violations), the noncompliance with security regulations raises doubt about an individual's trustworthiness, willingness, and ability to safeguard classified information.[(20)] The significance of a security violation does not depend on whether the information was actually compromised. It depends on the intentions and attitudes of the individual involved. The government established its case under Guideline K through Applicant's admissions and by showing that in April 2000, Applicant accessed a government classified network, copied classified information from the network, and removed it from its classified environment. He then copied the information, stored it in non-classified storage, shared with another individual, copied it into his laptop computer, and downloaded the classified information into a non-classified network. Applicant carried the information in his daily planner from April 2000 until February 2002. He also visited two foreign countries while having in his possession the classified information. Disqualifying

Condition (DC) 1: *Unauthorized disclosure of classified information*;[(21)] and Disqualifying Condition (DC) 2: *Violations that are deliberate or multiple or due to negligence*[(22)] apply.

Applicant had approximately nine years of experience working for the government and/or a government contractor prior to his mishandling of the classified information. He had access to classified information at the secret level since 1992, and at the SCI level since 1995. Applicant admitted he had received adequate training concerning his obligations while handling classified information. Considering his age, education, training, job responsibilities and experience handling classified information, he knew or should have known that the removal of classified information from a classified location was prohibited unless authorized by the custodian of the information, and in compliance with the rules for handling classified information.

Applicant took it upon himself to analyze the information he removed from the classified network, and to determine that it was okay for him to use it as he saw fit. He had no authority to classify any information for the government, or to decide whether the compromise of any or all of the information he compiled could cause harm to the government. Because of his professional experience, Applicant knew or should have known that even unclassified information may be considered classified when considered along with other relevant classified or unclassified information.

The fact that Applicant sought approval/confirmation from of his company manager concerning the removal of the data and his rationale for doing so shows he knew he was engaging in questionable behavior. Applicant was negligent by failing to request the data through proper security channels and/or to request a classification of the data. Furthermore, Applicant's concerns over "unanswered security questions that could cause him any unease during the (polygraph) interview" he was pending, show he knew he had engaged in questionable behavior and had placed himself in a precarious situation.

Applicant may have had good intentions/reasons for removing the information (i.e., improving the quality and response time of services provided to government agencies, and his personal convenience as well as that of his employer). Notwithstanding, his good intentions do not excuse his security violations. Considering the totality of the circumstances in his case, I find Applicant's violations were deliberate and/or due to his negligence. I also find Applicant knowingly violated the rules to store, transport, and use classified information. Either because his company did not have the facilities, or because it was convenient for him, he chose to mishandle the classified information.

With the exception of the behavior alleged in the SOR, there is no evidence Applicant has committed any other security violations. The evidence shows Applicant has a solid reputation for being an honest, dependable, and trustworthy individual. He has a solidly established reputation as a topnotch engineer with an excellent history of accomplishments developing cutting edge capabilities for the government. His security violations seemed the result of the hectic environment and the long hours he was working during a crucial period or time in his company. Nevertheless, those circumstances do not excuse his failure to exercise the degree of care that a reasonable person would have exercised under the same circumstances.

I specifically considered all Security Violations Mitigating Conditions (SV MC) and find only one applies, in part. As discussed above, Applicant's behavior was inadvertent.[(23)] Because of his age, education, training, an experience, he knew or should have known the removal of the data was against security policies and procedures, and he was aware of the consequences of his actions. Applicant's removal of the data, by itself, may be considered isolated since it seems it was done only in one occasion.[(24)] However, the mishandling of the information spanned almost two years, from April 2000 to February 2002. As such his mishandling of the classified information cannot be considered infrequent.[(25)]

Applicant argued he mishandled the information because of his lack of specialized training handling classified information and because he was taught it was proper for him to perform "data sanitation" (extracting only unclassified marked data from a larger set of data with several classifications). His arguments are not persuasive. By his own admissions, his employer provided him with adequate training.

I find Applicant's evidence demonstrates he had a positive attitude toward the discharge of security responsibilities. He also receives credit for following security procedures after confirming in 2002 that the data he removed was classified

(i.e., disclosed the security violation to his security manager and fully cooperated with the security investigation). SV MC 4: *Demonstrate a positive attitude toward the discharge of security responsibilities, applies.* Notwithstanding, considering the totality of the circumstances in his case, Applicant's favorable information is not sufficient to mitigate the Guideline K security concerns.

Under Guideline E, personal conduct is always a security concern because it asks the ultimate question - whether a person's past conduct instills confidence the person can be trusted to properly safeguard classified information. An applicant's conduct is a security concern if it involves questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations. Such behavior could indicate that the person may not properly safeguard classified information.[(26)]

The Guideline E allegations are based on the same factual incidents discussed under Guideline K. The government established its case under Guideline E by showing that Applicant violated the rules for handling classified information from April 2000 to February 2002. Disqualifying Conditions (DC) 5: *A pattern of . . . rules violations,*[(27)] applies.

I specifically considered all Guideline E Mitigating Conditions (MC), and for the same reasons outlined above under the discussion of Guideline K, incorporated herein, I conclude none of the MCs apply. Applicant's failure to follow security rules and procedures was deliberate. At best, he failed to exercise the degree of care and responsibility in the handling of the classified information expected from a prudent and reasonable person with his age, education, training, and experience handling classified information. Applicant's behavior demonstrate a serious lack of judgment, trustworthiness, and reliability. Guideline E is decided against Applicant.

I have carefully weighed all evidence, and I applied the disqualifying and mitigating conditions as listed under the applicable adjudicative guidelines. I specifically considered Applicant's age and experience, his outstanding performance of duty, his valuable contributions to the government, the lack of any misconduct or questionable behavior (except for the behavior alleged in the SOR), and his nine years working for defense contractors. Additionally, I gave Applicant credit for self-disclosing the security violation, for safeguarding the information after reporting the security violation, and for assisting the government to recover the data and identify the possible harm caused. On balance, I find Applicant's favorable information if not sufficient to mitigate the concerns created by his behavior. He violated the trust and confidence the government placed on him when he was granted access to classified information. His actions show Applicant cannot be trusted to follow the government's rules and procedures for handling classified information.

FORMAL FINDINGS

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

Paragraph 1, Security Violations (Guideline K) AGAINST APPLICANT

Subparagraphs 1.a(1) - 1.a(5) Against Applicant

Paragraph 2, Personal Conduct (Guideline E) AGAINST APPLICANT

Subparagraphs 2.a Against 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 Applicant. Clearance is denied.

Juan J. Rivera

Administrative Judge

1. *See,* Executive Order 10865, *Safeguarding Classified Information Within Industry* (Feb. 20, 1960, as amended, and Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (Jan. 2,

1992) (Directive), as amended.

2. Government Exhibit (GE) 3 (Applicant's answer to the SOR).

3. GE 4 (Letters of Recognition (dated November 14, 2001 and October 9, 2000; Commendation Correspondence, dated September 16, 1998 and October 3, 2000; Letter of Appreciation, dated December 11, 2000; and numerous outstanding performance appraisals for exceptional work rendered while employed by a government contractor.)

4. GE 6 and 7 (Office of Personnel Management Security Clearance Applications (SF86), dated October 23, 2003 and October 2002), unless indicated otherwise, are the source for the facts in this paragraph.

5. Applicant's answer to the FORM, dated February 16, 2007.

6. GE 10 (Applicant's statement, dated January 22, 2002), unless indicated otherwise is the source for the facts in the following paragraphs.). *See* also GE 5 (Applicant's November 25, 2003 statement), and GE 4 (Applicant's February 5, 2005 statement).

7. GE 4.

8. GE 10.

9. GE 8 (Applicant's company NISPOM's security violation report, dated September 24, 2002).

10. GE 5 (Applicant's November 2003 statement).

11. *Id.*

12. *See* Applicant's character reference letters attached to his answer to the FORM, and documents included in GE 4 (i.e., Letters of Recognition (dated November 14, 2001 and October 9, 2000; Commendation Correspondence, dated September 16, 1998 and October 3, 2000; Letter of Appreciation, dated December 11, 2000; and numerous outstanding performance appraisals for exceptional work rendered while employed by a government contractor.)

13. Directive, Section 6.3. Each clearance decision must be a fair and impartial common sense determination based upon consideration of all the relevant and material information and the pertinent criteria and adjudication policy in enclosure 2, including as appropriate:

14. Directive, E2.2.1. ". . . Available, reliable information about the person, past and present, favorable and unfavorable, should be considered in reaching a determination. . . ." The whole person concept includes the consideration of the nature and seriousness of the conduct and surrounding circumstances; the frequency and recency of the conduct; the age of the applicant; the motivation of the applicant, and the extent to which the conduct was negligent, willful, voluntary, or undertaken with knowledge of the consequences involved; the absence or presence of rehabilitation; and the probability that the circumstances or conduct will continue or recur in the future.

15. *See Department of the Navy v. Egan*, 484 U.S. 518, 531 (1988).

16. ISCR Case No. 98-0761 at 2 (App. Bd. Dec. 27, 1999) (Substantial evidence is more than a scintilla, but less than a preponderance of the evidence.); ISCR Case No. 02-12199 at 3 (App. Bd. Apr. 3, 2006) (Substantial evidence is such relevant evidence as a reasonable mind might accept as adequate to support a conclusion in light of all the contrary evidence in the record.); Directive, ¶ E3.1.32.1.

17. *Egan, supra* n.10, at 528, 531.

18. *See Id*; Directive E2.2.2.

19. *See* Exec. Or. 10868 § 7.

20. Directive, ¶ E2.A11.1.1.

21. Directive, ¶ E2.A11.1.2.1.

22. Directive, ¶ E2.A11.1.2.2.

23. Directive, E2.A11.1.3.1.

24. Directive, E2.A11.1.3.2.

25. Directive, E2.A11.1.3.2.

26. Directive, ¶ E2.A5.1.1.

27. *Directive, ¶ E2.A5.1.2.5.*