KEYWORD: Foreign Influence; Security Violations; Personal Conduct

DIGEST: Applicant's security violations and other exercises of poor operational security render him an unsuitable candidate for access to classified information. However, the record did not establish that Applicant was potentially vulnerable to foreign influence. Clearance denied.

CASENO: 05-01220.h1

DATE: 03/30/2007

DATE: March 30, 2007

In Re:	)	
	)	
----------	)	ISCR Case No. 05-01220
SSN: ----------	)	
	)	
Applicant for Security Clearance	)	
	)	

DECISION OF ADMINISTRATIVE JUDGE
JOHN GRATTAN METZ, JR

APPEARANCES

FOR GOVERNMENT
Francisco J. Mendez, Jr., Esquire, Department Counsel
D. Michael Lyles, Esquire, Department Counsel

FOR APPLICANT
Sheldon I. Cohen. Esquire

SYNOPSIS

Applicant's security violations and other exercises of poor operational security render him an unsuitable candidate for access to classified information. However, the record did not establish that Applicant was potentially vulnerable to foreign influence. Clearance denied.

STATEMENT OF THE CASE

Applicant challenges the 29 September 2005 Defense Office of Hearings and Appeals (DOHA) Statement of Reasons (SOR) recommending denial or revocation of his clearance because of foreign influence, security violations, and personal conduct.[1] Applicant answered the SOR 29 October 2005 and requested a hearing. DOHA assigned the case to me 20 March 2006, and I convened a hearing 4 May 2006. DOHA received the transcript 17 May 2006.

FINDINGS OF FACT

Applicant denied the SOR allegations, except for admitting foreign travel to Hong Kong and the People's Republic of China (PRC)(SOR 1.c. and 1.d.). He is a 46-year-old software engineer, employed by a defense contractor. He seeks reinstatement of the security clearance he previously held between October 1996 and October 2000, when he was terminated from his employment for cause.

Applicant—an ethnic Chinese—was born in Hong Kong in 1960, making him a citizen of the United Kingdom. He grew up in Hong Kong and was educated there. He immigrated to Canada in 1981, and to the U.S. in 1983. His parents also immigrated to the U.S. His father was a chef. His mother was a housewife. Applicant became a naturalized citizen in October 1995. His parents also became naturalized U.S. citizens; mother in June 1996, father in August 1996. On 1 July 1997, the United Kingdom lease on the British Crown Colony of Hong Kong expired and dominion, control, and the exercise of sovereignty over Hong Kong reverted to the People's Republic of China (PRC). Hong Kong will remain a Special Administrative Region (SAR) of the PRC, retaining a high degree of autonomy in all matters except foreign relations and defense, until 2047.

Applicant maintains minimal contact with Hong Kong. He remains in contact with a high school math teacher. They exchange emails about twice a year, and may meet for a meal whenever Applicant is in Hong Kong. Between 1998 and 2003, Applicant exchanged frequent emails with an electronic pen pal he met on a Hong Kong website. He met her briefly on one of his trips back to Hong Kong in December 1998. She married in 2003, and the frequency of their emails diminished until it stopped altogether. While Applicant's mother was alive, Applicant spoke monthly by telephone to a cousin who lived in the PRC. The conversations were largely about his mother and her health, and stopped after she died in June 2005. Until his mother died, Applicant's parents resided in Hong Kong for 2-3 months per year, usually in summer. They lived in a rented apartment. However, Applicant's father is now 73, and his health prevents him from traveling to Hong Kong alone. The lease on the apartment expired in March 2006 and his father did not renew it. He lives most of the year with Applicant, but resides with Applicant's older brother in Canada during part of the year.

Applicant was briefly married to a PRC national from Hong Kong. They met in 2000 through a personals advertisement in a Hong Kong newspaper, and communicated for several months by

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

telephone and email. In June 2000, he flew to Hong Kong to meet her and her family, then they embarked on a two-week, pre-wedding honeymoon to Japan and Europe. She immigrated to the U.S., where they were married in September 2000. They separated 4½ months later, ostensibly because of her videotaped unfaithfulness. They were divorced in February 2002.

Applicant has traveled to Hong Kong on a number of occasions, and for a variety of reasons, since 1997. In June 1997 he traveled to Hong Kong to visit family and friends. He did so again in December 1998, and met his email pen pal in person. He traveled to Hong Kong in June 2000 to meet his prospective bride and take her on a pre-marriage honeymoon trip. In December 2001, he returned to Hong Kong with his mother—and traveled to the PRC as well—so she could visit with family. Finally, he traveled to Hong Kong in December 2005 to visit friends.

On 10 October 2000, Applicant was terminated from employment after being debriefed from access to classified information by the defense contractor for whom he had worked since September 1996. A number of security concerns lead to his termination. On 18 September 2000, six days after his marriage, Applicant sent three classified files by unclassified email to another defense contractor working on the same project. The security violation was discovered almost immediately, and both companies took quick action to ensure that the classified files had not been compromised, ultimately concluding that the risk of compromise was minimal (G.E. 6).

The ensuing investigation disclosed the component violations in the incident: improperly copying classified information from the classified computer, improperly loading the classified information onto an uncontrolled disk,[2] improperly transferring classified data from one system to another,[3] and improperly transmitting classified materials (G.E. 4). Applicant has variously ascribed the violation to "the pressure of the deadline and no one around to help me and the manager was (sic) on vacation (G.E. 2)," to not being informed by the company that he could not transmit classified information by unclassified email and worrying about his fiance's situation (G.E. 7,[4] Answer), to a general lack of training (Tr. 154). However, he acknowledged that he knew he should not send classified information over the internet (Tr. 94). Further, company records reflect that Applicant attended a week-long security awareness seminar—required of every employee with a security clearance—in November 1999.[5]

[2]"Uncontrolled" meaning not properly marked with the classification of the data contained on the disk and not bringing the disk into the accountability system for handling classified information.

[3]From a classified computer to an unclassified computer.

[4]He stated "I had to decide whether to get married in a week." However, Applicant was already married when the violation occurred.

[5]The Facility Security Officer at Applicant's company testified that Applicant's attendance was confirmed by an entry in the company's security database. The entry in the database was based on Applicant's signing in at the seminar (Tr. 204). She further testified that every employee gets trained on the company's information security program before they are given a company email account (Tr. 193).

As a result of this security violation, Applicant received remedial training, which consisted of verbal counseling by his laboratory security officer[6] on the proper handling procedures, security office personnel also reviewing the proper procedures with him, and providing him with his personal copy of the information security manual (to be thoroughly reviewed), among other measures. Applicant acknowledged that he received the manual, but testified that he did not review it because of the press of other business. During the course of the investigation, Applicant did not claim that he had received inadequate training (Tr. 193). Further, both his laboratory manager and a laboratory co-worker indicated that Applicant was aware of the requirements for handling and transmitting classified information (G.E. 10).

On 26 September 2000, eight days after his first violation, Applicant committed essentially the same violation in the laboratory. He needed to print the program code from the classified computer he was working on.[7] However, the classified computer did not have a printer attached to it. So Applicant again copied the information he needed and loaded it onto another uncontrolled disk. He intended to put the disk into another classified computer in the laboratory that had a printer. However, his improper copying of the files was discovered before he could complete his task.[8] The company considered this the second security incident within a ten day period (G.E. 8), and Applicant was removed from access to the company's classified areas. On 6 October 2000, he was debriefed from the classified program he was working on.

The ensuing investigation uncovered additional security-related anomalies regarding Applicant. The company discovered that Applicant's most recent clearance application incorrectly listed his parents' places of birth as his residence address in the U.S. (instead of the PRC and Hong Kong), and listed his and his brother's place of birth as his residence address in the U.S. (instead of Hong Kong).[9] The company also decided it would be a prudent security measure to examine Applicant's email account on his unclassified computer to ensure that no other classified information had been improperly sent out. None had, but the company discovered that Applicant had forwarded sensitive emails to many associates, both U.S. and foreign, including the woman he had just married. Applicant's emails disclosed that he worked in a classified lab and described details of his job and the contracts he worked on, information sensitive to the company. The emails also contained

---

[6]At the time of the security violation, Applicant worked in a specific laboratory for his employer (of many run by the employer at the same location). Each laboratory had an information security representative—a regular laboratory member who had received additional training in information security to serve as a focal point for questions arising in the laboratory.

[7]According to Applicant, the software program code is unclassified, but the database the program is supposed to run is classified. This results in the computer being a classified computer, at the highest level of classification of any of the information in the database.

[8]Applicant claimed he did load the files into the other computer and print the code, contrary to the company's recorded version of the events. I find the company's version more credible, both because the company recorded the events more-or-less contemporaneously and because the company designated this incident a "practice dangerous to security" rather than a security violation—a distinction it made because the files on the disk were not downloaded to another system or transmitted (Tr. 194).

[9]The company considered this a falsification of his clearance application. Applicant attributed the mistake to his inability to read the fine print on the application, so when he saw "city, county, country," he assumed he should fill in the place of residence (G.E. 9). I find his explanation implausible, because his brother lives in Canada, not with Applicant.

documents and slide shows from his program manager (G.E. 5).[10] Additionally, there were emails between Applicant and his fiancé that raised suspicions about the legitimacy of the marriage.[11] The cumulative effect of these discoveries, coupled with the two security incidents, was that Applicant was terminated from his job on 10 October 2000.[12]

Applicant's character references, who include his father, his pastor, a friend, and two previous supervisors, consider Applicant an honest and trustworthy individual. They believe he can be trusted to handle classified information. However, these favorable references must be compared against the unfavorable references developed during his background investigation (G.E. 10), which call into question his suitability for access to classified information.[13]

The PRC is a repressive, totalitarian government with foreign policy goals antithetical to the U.S., although it has cooperated with the U.S. in the global war on terrorism in recent years. It has an active, effective intelligence service that targets U.S. intelligence and economic information, and operates against its citizens in the U.S. However, Hong Kong operates as an SAR of the PRC, with substantial independence until at least 2047.

POLICIES AND BURDEN OF PROOF

The Directive, Enclosure 2 lists adjudicative guidelines to be considered in evaluating an Applicant's suitability for access to classified information. Administrative Judges must assess both disqualifying and mitigating conditions under each adjudicative issue fairly raised by the facts and circumstances presented. Each decision must also reflect a fair and impartial common sense

[10]The company FSO described emails discussing diagrams, software, censor fusion information, and program management reviews—all of which considered proprietary information (Tr. 197-198).

[11]Applicant attempted to portray an email concerning payment as merely a discussion of a dowry. However, the circumstances of Applicant's marriage are unusual at best. Applicant described it as similar to a mail-order bride, however, he has not addressed the internal inconsistencies raised by the speed with which he decided to marry, then became so suspicious of her fidelity that he thought it prudent to have her investigated, caught her on videotape, and separated 4½ months after their marriage.

[12]Applicant minimized the circumstances of his termination on his May 2003 clearance application (G.E. 2). Instead of revealing that he was terminated or fired from this job, he stated only that he "left a job for other reasons under unfavorable circumstances." Similarly, instead of revealing that he improperly transmitted classified files, he stated only that "I sent out some files to the client by mistakes (sic) . . ." He also minimized the circumstances of his termination during his July 2003 subject interview (G.E. 7). During his initial questioning by the investigator, Applicant disclosed only the improper transmission of files. Only in response to further prodding by the investigator did he disclose that the files were classified (Tr. 244-247).

[13]In his clearance application (G.E. 2), Applicant listed his laboratory supervisor and a co-worker as two people who could confirm his claim that he had done nothing "malicious" by transmitting the files by mistake. Indeed, both references stated their belief that Applicant did not act maliciously. However, both confirmed that Applicant had been properly trained regarding his responsibility for handling classified information. His supervisor noted Applicant was aloof, and had demonstrated poor judgment and a lack of attention to detail on several occasions regarding classified information. His co-worker stated Applicant did not perform his tasking satisfactorily, and described him as absent-minded and generally not a good fit for the position he was in (G.E. 10). His supervisor in his next job in 2000, which did not require a clearance, voiced concerns about Applicant's ability to work with very sensitive classified information because of the emotional state he exhibited during his divorce and his tendency to be talkative on the job (G.E. 10).

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 for or against Applicant. However, specific adjudicative 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. Considering the SOR allegations and the evidence as a whole, the relevant, applicable, adjudicative guidelines are Guideline B (Foreign Influence), Guideline K (Security Violations), and Guideline E (Personal Conduct).

Security clearance decisions resolve whether it is clearly consistent with the national interest to grant or continue an Applicant's security clearance. The government must prove, by something less than a preponderance of the evidence, controverted facts alleged in the SOR. If it does so, it establishes a *prima facie* case against access to classified information. Applicant must then 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.

Persons with access to classified information enter into a fiduciary relationship with the government based on trust and confidence. Therefore, the government has a compelling interest in ensuring each Applicant possesses the requisite judgement, reliability, and trustworthiness of those who must protect national interests as their 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.[14]

CONCLUSIONS

The government failed to establish a case for disqualification under Guideline B. Applicant's travel to Hong Kong (SOR 1.c.) and the PRC (SOR 1.d.) has no independent security significance. At best, the travel might demonstrate ties of affection or obligation to someone living in either country.[15] Further, Applicant's contacts with his cousin in the PRC (SOR 1.b.) and his parents' contacts with Hong Kong (SOR 1.e.) lack meaningful security significance because he has had no contact with his cousin (who is also not an immediate family member) since his mother died in June 2005, and his father is unable to travel to Hong Kong and no longer leases an apartment there. Similarly, Applicant no longer has any contact with his email pen pal in Hong Kong (SOR 1.a.). What remains is Applicant's semi-annual emails to his old high school math teacher and their occasional meals together when Applicant visits Hong Kong. The longevity of the relationship argues for its closeness. However, the nature and extent of the contacts otherwise argues against finding that the contacts meet the threshold for ties of affection or obligation.

The plain language of the stated concerns and disqualifying factors of Guideline B may (or may not) raise concerns and may (or may not) be disqualifying. This implies that mere citizenship of, or residence in, a foreign country of a person with close ties of affection or obligation to Applicant does not automatically establish the disqualifying conditions precedent to shift the burden

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

[15]E2.A2.1.2.1. An immediate family member, or a person to whom the individual has close ties of affection or obligation, is a citizen of, or resident or present in, a foreign country;

to Applicant to mitigate the government's case. In this case, the evidence does not support a conclusion that Applicant has any such ties. I resolve Guideline B for Applicant.

However, the government established a case for disqualification under Guideline K by demonstrating that Applicant committed deliberate security violations during October 2000,[16] when he twice improperly downloaded classified information and once improperly transmitted classified files.[17] He also, for some period before October 2000, deliberately violated company security regulations by transmitting proprietary information to individuals with no need for the information.

Most of the mitigating conditions are inapplicable to Applicant. The security violations were deliberate.[18] The security violations were arguably isolated or infrequent, but the violations of company regulations regarding proprietary information were more extensive.[19] Applicant had been properly and regularly trained on the security requirements of his positions.[20] Finally the Applicant's current behavior fails to demonstrate a positive attitude towards the discharge of his security responsibilities.[21] He has consistently denied responsibility for his security violations, asserting a lack of training. He has consistently minimized the severity of the two October 2000 violations, which is emphasized by the speed with which the company first investigated the conduct, then acted to debrief Applicant and ultimately terminate his employment. These are not the actions of a company who viewed Applicant's conduct as harmless.

Further, Applicant has consistently sought to draw artificial distinctions between various degrees of security violations based on a narrow focus on the characterizations used in conducting security violation investigations. The National Industrial Security Program Operating Manual (NISPOM), January 1995, defines "security violation" as a "failure to comply with the policy and procedures established by this Manual that reasonably could result in the loss or compromise of classified information." Applicant's two security incidents in October 2000 satisfy this definition notwithstanding that the company characterized the first as a "violation" because classified information was removed from the laboratory, and the second as a "practice dangerous to security" because the classified information was intercepted before it could be lost or compromised. A "practice dangerous to security" was still considered a violation of the rules and regulations (Tr. 195). In addition, Guideline K does not confine itself to security regulations that deal only with the handling of classified information. Security regulations can, and do, deal with safeguarding official use or privacy act material, as well as with operational security—which deals with safeguarding otherwise unclassified and unrelated pieces of information that may have security significance in the aggregate. Internally, defense contractors, as here, may have security regulations regarding use and

---

[16]E2.A2.11.1.2.2. Violations that are deliberate or multiple or due to negligence.

[17]E2.A2.11.1.2.1. Unauthorized disclosure of classified information;

[18]E2.A2.11.1.3. Conditions that could mitigate security concerns include actions that: E2.A2.11.1.3.1. Were inadvertent;

[19]E2.A2.11.1.3.2. . . .Were isolated or infrequent;

[20]E2.A2.11.1.3.3. . . .Were due to improper or inadequate training;

[21]E2.A2.11.1.3.4. . . .Demonstrate a positive attitude towards the discharge of security responsibilities.

dissemination of company proprietary information. Violations of any of these varied kinds of security regulations raises doubts about an applicant's willingness and ability to safeguard classified information. Indeed, it would be anomalous to suggest that an individual who had never been cleared, but who had violated his employer's requirements for safeguarding information in other areas, could not have his case adjudicated under Guideline K. I resolve Guideline K against Applicant.

Finally, the government established a Guideline E case by demonstrating Applicant's questionable judgment in executing his security responsibilities over an extended period of time.[22] While his violations of the NISPOM were confined to October 2006, his violation of company regulations covered a greater period of time.[23] In addition, he minimized his conduct, both on his clearance application and during his subject interview.[24]

Applicant meets none of the mitigating conditions under personal conduct. His conduct was substantiated and pertinent to a judgment determination.[25] His misleading description of his termination, both on his application and during his subject interview was neither isolated nor distant.[26] He did not disclose the full circumstances of his termination until pressed by the investigator during the subject interview.[27] Nor did Applicant receive bad advice about what adverse information he should reveal.[28] I resolve Guideline E against Applicant.

FORMAL FINDINGS

[22]E2.A5.1.2.1. Reliable unfavorable information provided by associates, employers, coworkers, neighbors, and other acquaintances;

[23]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;

[24]E2.A5.1.2.3. Deliberately providing false or misleading information concerning relevant and material matters to an investigator, security official, competent medical authority, or other official representative in connection with a personnel security or trustworthiness determination;

[25]E2.A5.1.3.1. The information was unsubstantiated or not pertinent to a determination of judgment, trustworthiness, or reliability;

[26]E2.A5.1.2.2. The falsification was an isolated incident, was not recent, and the individual has subsequently provided correct information voluntarily;

[27]E2.A5.1.2.3. The individual made prompt, good-faith efforts to correct the falsification before being confronted with the facts;

[28]E2.A5.1.2.4. Omission of material facts was caused or significantly contributed to by improper or inadequate advice of authorized personnel, and the previously omitted information was promptly and fully provided;

Paragraph 1. Guideline B: FOR APPLICANT

Subparagraph a: For Applicant
Subparagraph b: For Applicant
Subparagraph c: For Applicant
Subparagraph d: For Applicant
Subparagraph e: For Applicant

Paragraph 2. Guideline K: AGAINST APPLICANT

Subparagraph a: Against Applicant
Subparagraph b: Against Applicant

Paragraph 3. Guideline E: AGAINST APPLICANT

Subparagraph a: Against Applicant
Subparagraph b: 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 denied.

John G. Metz, Jr.
Administrative Judge