DATE: September 29, 2003

In re:

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

Applicant for Security Clearance

CR Case No. 01-20562

REMAND DECISION OF ADMINISTRATIVE JUDGE

ROGER C. WESLEY

APPEARANCES

FOR GOVERNMENT

Department Counsel, Katherine A. Trowbridge

FOR APPLICANT

Herbert M. Silverberg, Esq.

SYNOPSIS

Applicant established and maintained Internet contacts with foreign women (five in all) on his home computer over several years; none of these contacts exhibited any indications of being foreign intelligence agents, or individuals interested in targeting Applicant for information about his work or company. Nor is there evidence of monitoring of Applicant's Internet communications by agents of foreign powers interested in targeting Applicant for foreign intelligence collection. Applicant's imputed knowing and wilful omissions of his three covered foreign contacts in his SF-86 and initial DSS interview were promptly corrected within minutes and qualify as prompt, good faith disclosures. Applicant is highly regarded by his employer as a person who is reliable and trustworthy and establishes his overall trustworthiness necessary to retain his security clearance. Clearance is reaffirmed on remand.

PROCEDURAL ISSUES

At hearing, the Government moved to amend sub-paragraph 1.a of the SOR to insert the words **you admitted** you deliberately falsified material facts when you failed to disclose your foreign contacts . . . . . There being no objection from Applicant and good cause being demonstrated, the Government's amendment request was granted. Applicant's answer was unchanged by the amendment.

By its remand order of August 28, 2003, the Appeal Board remanded the case to resolve two issues: whether or not Department Counsel's e-mail message of February 14, 2003, with an attached article posted on the Internet, was copied Applicant's counsel, and whether or not Applicant's counsel had the opportunity to object or otherwise respond to the article.

On receipt of the remand article, I faxed a letter (on September 3, 2003) to counsel for the parties asking them to address these issues. Both parties responded to my letter the following day: Applicant confirmed he had not received a copy of the e-mail, and Department Counsel confirmed she had not copied Applicant with the e-mail message and attached article.

Applicant did not respond to the text of the article with any additional information or comments within the 14 days provided.

For good cause shown, the article is admitted as exhibit 4. While the article is essentially hearsay, it is made available publicly on the Internet and subject to challenge. Given its general availability and the more relaxed hearsay standard recognized in DOHA administrative proceedings, it may be admitted for the weight deserved. By its acceptance, however, the article's probative value may not be assigned the same force and effect reserved for published articles and works that warrant official notice under Rule 201(b) of F.R.Evid.

STATEMENT OF THE CASE

On August 12, 2002, the Defense Office of Hearings and Appeals (DOHA), pursuant to Executive Order 10865 and Department of Defense Directive 5220.6 (Directive), dated January 2, 1992, issued a Statement of Reasons (SOR) to Applicant, which detailed reasons why DOHA could not make the preliminary affirmative finding under the Directive that it is clearly consistent with the national interest to grant or continue a security clearance for Applicant, and recommended referral to an administrative judge to determine whether clearance should be granted, continued, denied or revoked.

Applicant responded to the SOR on September 27, 2002, and requested a hearing. The case was assigned to this Administrative Judge on October 30, 2002. Pursuant to notice, a hearing was convened on November 13, 2002, for the purpose of considering whether it would be clearly consistent with the national interest to grant, continue, deny or revoke Applicant's security clearance. At hearing, the Government's case consisted of three exhibits; Applicant relied on two witnesses (including himself) and two exhibits. The transcript (R.T.) of the proceedings was received on November 21, 2002.

STATEMENT OF FACTS

Applicant is a 36-year old associate software engineer for a defense contractor who seeks a security clearance.

Summary of Allegations and Responses

Applicant is alleged in the SOR to have deliberately falsified a signed, sworn statement given to a DSS agent in July 2001 by failing to disclose his foreign contacts with multiple foreign citizens through Internet chat rooms and ICQ . Applicant's alleged Internet chats include "cyber-sex" with foreign citizens and revelations of his software engineer employment at a US military base.

For his response to the SOR, Applicant denied generally being a security risk while admitting specifically to not disclosing his foreign Internet contacts (albeit, without knowledge his omissions were material and without any past experience in the security experience process). Applicant admitted to engaging in Internet chats, including cyber-sex with foreign citizens, and to probably telling some of these contacts about his unclassified work and position with his company.

Relevant and Material Factual Findings

The allegations covered in the SOR and admitted to by Applicant are incorporated herein by reference adopted as relevant and material findings. Additional findings follow.

Applicant in 1995 began using the Internet to facilitate chats with foreign citizens through an instant messaging system known as ICQ.[(1)] To get started with an ICQ software program, a prospective user need only register, get an ICQ handle (or nickname) and fill in certain details; so that other ICQ users can recognize the user and communicate with him.

When Applicant registered to use ICQ in 1995, he adopted Spartacus as his identifying "handle." He initiated his Internet contacts while he was a student in college (*i.e.,* in 1995). In these Internet contacts, he met a Canadian user (Ms. A) sometime in 1998, who he described as a married woman in her late 40s (*see* ex. 2). He maintained his Internet contacts with Ms. A for two to three years he estimates. No identified cyber-sex communications were included in this chat

relationship. Lonely and introvertish by nature, Applicant built on his Internet contacts with Ms. A and eventually accepted her offer to meet her family in Canada. Disappointed with his two-week visit to her home, he ceased further contact with her on his return home.

Applicant's second Internet contact was with a person (Ms. B, a resident of Puerto Rico) he met in an ICQ introduction in 1999. He arranged a personal meeting with her on a trip he made to Europe in 2000 with his mother and brother to visit his grandmother (*see* ex. B; R.T., at 117-19). Ms. B was 34 to 35 years in age and in an unhappy marriage, when he met her in France. Following a brief sexual affair with Ms. B, Applicant became disappointed with the experience, cut back his Internet contacts with her on his return to the US, and terminated his relationship with her altogether before beginning his current employment in May 2001.

Applicant continues to pursue Internet contacts with foreign women. One (Ms. C), a divorced woman in her mid 30s, he communicates with, but has no cyber-sex with her (*see* exs 2 and B; R.T., at 115). Another (Ms. D) is an 18-year old college student he has been communicating with on the Internet since 1996. With Ms. D, he began engaging her in cyber-sex in 1996 while he was a college student: He later came to learn she was just 13 years of age when he first engaged in cyber-sex with her. He continues to maintain contact with Ms. D and looks forward to someday meeting her in person (*see* ex. 2; R.T., at 113-14). Both women know that Applicant is a soft ware engineer employed by a US defense contractor.

Besides his identified Internet chats, Applicant has visited ICQ rooms with a sexual theme. Most of his visits have been brief ones lasting no more than a month or two. Applicant does recall having a private exchange with a woman (Ms. E) in one of these chat rooms he identifies as a "multi-city" site. For a two month period in the Fall of 2000, he exchanged cyber-sex messages with her on a daily basis (*see* ex. 2). Applicant estimates to have exchanged cyber-sex communications with 5 to 6 different women since his first encounter in 1995.

In the past, Applicant has experienced periodic bouts with depression. These depression experiences were particularly severe in 1995. They are attributed to his seeking escape from his experiences and feelings of sadness, worthlessness, and a sense of wasted time.

Dr. F (a credentialed board certified psychiatrist) who evaluated Applicant in September 2002 detailed Applicant's psychiatric history, which included occasional bouts of depression and panic attacks (ex. B). Dr. F diagnosed Applicant to have an introverted personality with a dysthymic (mood) disorder that is currently relatively mild and personality traits that represent "an enduring pattern of inner experience and behavior that deviates from expectations of his culture" (*see* ex. B; R.T. , at 46-47). Dr. F characterizes Applicant as a person who does not enjoy close relationships, but prefers solitary activities and lacks close friends. Tracing Applicant's cyber-sex activities on the Internet, Dr. F found no historical or clinical data evidencing any sexual or gender identity disorders. Dr. F's concluded prognosis for Applicant was fair without treatment, and good with treatment designed to deal with his depression and improve his interpersonal relationships. Dr F was impressed that Applicant was scaling back his Internet contacts, finding it more and more to represent a waste of his time and energies (*see* ex. B; R.T., at 51-52, 60).

Applicant was asked to complete a SF-86 in May 2001. In none of the questions he responded to did he disclose his foreign Internet contacts. However, none of the pertinent questions covering foreign contacts in his SF-86 specifically asked him to address any of his foreign Internet contacts. Question 9 asked about his relatives and associates. While the word associates is not defined on the face of the SF-86, it can certainly encompass several meanings: business relationships foremost, but also companions and comrades. *See Webster's Ninth New Collegiate Dictionary* (1984 ed.). Foreign contacts with whom Applicant has unbroken regular Internet contact (like three of the five foreign contacts he identified in his signed, sworn statement as persons he still stays in touch with) could be considered associates and persons, as such, that should be identified when responding to question 9. This is not to suggest that any person an Internet user might choose to chat with in an ICQ setting should be characterized as an "associate." It only means that persons with whom the ICQ user establishes regular intimate contact may be considered an associate who should be disclosed when responding to the question asking about the applicant's relatives and associates.

Government, though, seeks a much broader reading of the term "associates" used in question 9 of Applicant's SF-86: one expansive enough to include prior, but since terminated relationships. By this logic, a responder would be required to list his or her foreign relationships dating from birth. Such a reading is neither apparent nor compatible with interpretations of common sense. Applicant, accordingly, is excused from listing his prior foreign relationships, with whom he has long since ceased communicating. Still, Applicant claims he had no understanding at the time he was answering his SF-86 that he was required to disclose even his remaining three foreign contacts with whom he maintains ICQ connections. Believing their identities were not material to a clearance determination, he did not list them. At issue is whether his claims are credible, taking into account all the circumstances known at the time.

Tangentially, Applicant was provided some notice of the Government interest in his current foreign contacts in the very specifically worded questions 11 through 16. Each of these questions address respective areas of foreign military participation, foreign property and employment, holding a foreign passport, and foreign countries visited in considerable detail. In responding to these questions, Applicant did list his trips to Canada, France and Germany between 1999 and 2000. But while some credit may be given to Applicant's not understanding everything called for in question 9, his assigned reasons for not being forthcoming about the bulk of the information covered are more persuasively explained in his later signed, sworn statement: embarrassment, fear of being perceived as a loser, and concern over being perceived that he was trying to hide the information about his foreign contacts (*compare* ex. 2 with R.T., at 104-05 and Applicant's answer). Considering Applicant's education, intelligence and job stature with his employer, his omissions may be best characterized as a rationalized attempt to avoid mention of contacts and activities he was not comfortable in discussing with Government representatives. To the extent his omissions of these contacts were not clearly the result of mistaken understanding, adverse inferences of knowing and wilful withholding of pertinent information cannot be averted.

When first interviewed by a DSS agent in July 2001, Applicant was asked whether the information he certified to in his SF-86 was correct, and he answered affirmatively (*see* R.T., at 97). The agent then asked him a series of questions about his citizenship, foreign contacts and foreign travel, which were not of a confrontational nature. In response to the agent's questions, Applicant reiterated his trips to France and Canada, which he described as trips to see family members, before finally telling the agent about his Internet liaison with his Canadian Internet contact (R.T., at 100-02). At this point, Appellant advised the agent he wished to end the interview, which terminated. (*see* R.T., at 82-84). Whatever the relevance of this information, he did not wish to get into it.

Just after ending his first DSS interview, Applicant had a change of heart after talking with his mother, and called the agent back to reconvene the interview (*see* R.T., at 85). In this convened second interview convened on the same day, Applicant was very cooperative with the agent and signed a statement providing the full details of his previously omitted foreign Internet contacts with the five covered individuals, along with his reasons for his previous omissions: embarrassment, fear of being perceived as a loser, fear over being perceived as trying to hide something (*see* ex. 2). By Applicant's accounts and fair reading of his July 2001 signed, sworn statement, his admissions bear no indicia of statements produced by confrontation by the interviewing DSS agent (*compare* ex. 2 with R.T., at 85-88). Applicant may be credited, accordingly, with providing the pertinent foreign contact information promptly (within two months of executing the SF-86) and voluntarily.

Applicant is highly regarded by his direct supervisor (X) who describes him as dependable, trustworthy and honest. X has some 20 engineers working for her, most of whom are not known to acknowledge any mistakes in their assignments, like Applicant is known for (*see* R.T., at 125). Applicant has consistently received excellent performance evaluations. X, who sees him daily, credits him with being forthcoming about his Internet connections (to include cyber-sex) with foreign nationals. Familiar with the practice through her supervisioral interfacing with others in her line of authority, she has had no reports of any kind of security compromise from chat room exchanges like Applicant's (*see* R.T., at 130). Notwithstanding the allegations and Applicant's acknowledgment of his covered Internet contacts, X continues to believe he is a valued employee who can be entrusted to safeguard classified information (*see* R.T., at 131).

POLICIES

The Adjudicative Guidelines of the Directive (Change 4) list "binding" policy considerations to be made by Judges in the decision making process covering DOHA cases. The term "binding," as interpreted by the DOHA Appeal Board, requires the Judge to consider all of the "Conditions that could raise a security concern and may be disqualifying" (Disqualifying Conditions), if any, and all of the "Mitigating Conditions," if any, before deciding whether or not a security clearance should be granted, continued or denied. The Guidelines do not require the Judge to assess these factors exclusively in arriving at a decision. In addition to the relevant Adjudicative Guidelines, judges must take into account the pertinent considerations for assessing extenuation and mitigation set forth in E.2.2 of the Adjudicative Process of Enclosure 2 of the Directive, which are intended to assist the judges in reaching a fair and impartial common sense decision.

Viewing the issues raised and evidence as a whole, the following adjudication policy factors are pertinent herein:

Personal Conduct

Basis: conduct involving questionable judgment, untrustworthiness, unreliability, or unwillingness to comply with rules and regulations could indicate that the person may not properly safeguard classified information.

Disqualifying Conditions:

DC 2 The deliberate omission, concealment, falsification or misrepresentation of relevant and material facts from any personnel security questionnaire, personal history statement or similar form used to conduct investigations, determine employment qualifications, award benefits or status,

determine security clearance eligibility or trustworthiness, or award fiduciary responsibilities.

DC 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.

DC 4 Personal conduct or concealment of information that increases an individual's vulnerability to coercion, exploitation or duress.

Mitigating conditions:

DC 2 The falsification was an isolated incident, was not recent, and the individual has subsequently provided correct information voluntarily.

DC 3 The individual made prompt, good-faith efforts to correct the falsification before being confronted with the facts.

DC 5 The individual has taken positive steps to significantly reduce or eliminate vulnerability to coercion, exploitation

or duress.

Burden of Proof

By virtue of the precepts framed by the Directive, a decision to grant or continue an Applicant's request for security clearance may be made only upon a threshold finding that to do so is clearly consistent with the national interest. Because the Directive requires Administrative Judges to make a common sense appraisal of the evidence accumulated in the record, the ultimate determination of an applicant's eligibility for a security clearance depends, in large part, on the relevance and materiality of that evidence. As with all adversary proceedings, the Judge may draw only those inferences which have a reasonable and logical basis from the evidence of record. Conversely, the Judge cannot draw factual inferences that are grounded on speculation or conjecture.

The Government's initial burden is twofold: (1) It must prove any controverted fact[s] alleged in the Statement of Reasons and (2) it must demonstrate that the facts proven have a material bearing on the applicant's eligibility to obtain or maintain a security clearance. The required showing of material bearing, however, does not require the Government to affirmatively demonstrate that the applicant has actually mishandled or abused classified information before it can deny or revoke a security clearance. Rather, consideration must take account of cognizable risks that an applicant may deliberately or inadvertently fail to safeguard classified information.

Once the Government meets its initial burden of proof of establishing admitted or controverted facts, the burden of persuasion shifts to the applicant for the purpose of establishing his or her security worthiness through evidence of refutation, extenuation or mitigation of the Government's case.

CONCLUSIONS

Applicant is a highly regarded software engineer who as an adolescent shied from close relationships. To address his periodic bouts with depression he turned to the Internet's ICQ. Through ICQ chat room contacts on his home computer, Applicant found personal expression through visits to online chat rooms. Some of these contacts evolved into cyber-sex relationships with foreign women of widely varying ages.

Using a fictional handle for identification purposes when entering an ICQ chat room, Applicant established online relationships with eight or more different foreign women, beginning in 1995. Of these established Internet relationships, five to six of these involved cyber-sex exchanges, three of which he recalls to be of a repeated nature (*i.e.,* his exchanges with B, D and E). Of these cyber-sex relationships, only one produced a physical sexual encounter, which was brief and not repeated. Applicant does continue to maintain cyber contacts with two foreign women through the same online chat room he has been affiliated with since 1995: one that includes sexual content and one that does not..

Government claims Applicant's cyber-sex online relationships with foreign women increase his vulnerability to coercion, exploitation and duress, without regard to country origin of his foreign contacts. For support, Department Counsel cites to an article entitled *The Honeypot and Sexpionage* (covered in DoD's Adjudicated Desk reference) as a good source of the type of security concerns that typically accompany Internet visits to putative "romantic sites." While certainly legal and not immoral by secular public policy standards, they provide rich outlets for intelligence opportunists and agents for identifying new targets for exploitation. *See Adjudicators Desk Reference* (identified at hearing) and the article itself admitted as exhibit 4.

Because one or more persons listening in on the chat site might be an agent for an adversary or competitor, individual chat room users like Applicant are always exposed to having their conversations monitored and potentially exploited for intelligence purposes. Under such circumstances, even though a user's cyber-sex partner might himself or herself be innocent, the monitoring agent of a foreign power might be provided with useful intelligence information from the chat participants. It is not unusual either for an intelligence agent from a foreign power to offer sexual favors in return for information. Foreign agents are known to be people fluent in the language of the targeted individual and who typically pose as college professionals or graduate students majoring in computer science or electrical engineering. *See Honeypot and Sexpionage* article.

Notwithstanding the scarcity of evidence linking Applicant to any threatened compromise associated with his Internet chat room activity, Applicant is of record admitting he never inquired much into the background of the foreign contacts he has communicated with, relying on his knowledge of the Internet and gut instincts. To be sure, he still stays in contact with three of the foreign women he met. While some of these contacts may know his professional status, none know anything about the nature of his work. His identified Internet relationships (even the ones that involved cyber-sex and physical sex) do not appear to have involved any intelligence agents or sources of foreign powers with interests inimical to the security interests of the US. Any potential espionage linkage to Applicant's Internet activities remain unproven. Applicant's chat room contacts do not involve the use of a classified hard frame either. Moreover, all but three of his foreign relationships have since abated and present no known current espionage risks that can be identified and gauged. Under these circumstances, Applicant may invoke MC 5 (positive steps to reduce or eliminate vulnerability to coercion, exploitation or duress) of the Adjudicative Guidelines for personal conduct.

Applicant himself is a very introverted individual who is not as a rule given to exchanging information about his company and work. While so private a person might be more apt to withhold important information from government investigators seeking to enlist material information from him, he has been candid about his relationships once their importance was explained to him.

Balancing the security risks of Netspionage by foreign Internet contacts associated with Applicant's communications with foreign women in ICQ chat rooms with Applicant's otherwise lawful and not immoral Internet behavior (with the lone exception of his engaging in cyber-sex with the Internet contact he later came to learn was just 13), Applicant's actions must be concluded to be activities covered by manageable risk. This is not to say that such Internet chats with foreign persons could not produce unacceptable security risks in certain identified situations. The Government certainly need not wait for a compromise of classified information to occur before it is entitled to take preemptive steps to address the identified risk in the covered activity. *Cf. Adams v. Laird,* 420 F.2d 230, 238-39 (DC Cir. 1969), *cert. denied,* 397 U.S. (1970). But this risk threshold is not yet present in Applicant's situation. No evidence is available to indicate that any of Applicant's foreign contacts were foreign intelligence agents targeting Applicant for information of a classified or proprietary nature, or that there were foreign intelligence agents monitoring Applicant's communications. Actual evidence of either of the foregoing would change the whole dynamic of the behavior at issue.

Taking into account all of the evidence and competing theories of security risk associated with Applicant's foreign Internet contacts, both past and present, Applicant succeeds in both eliminating and reducing any vulnerability he might have to coercion, exploitation and duress to manageable levels of risk compatible with his holding a security clearance. Favorable conclusions warrant with respect to the allegations covered by sub-paragraph 1.b. of Guideline E.

Posing potentially serious security concerns as well are Applicant's omissions of his foreign Internet chats from both question 9 of his SF-86 and his initial July 27 2001 DSS interview. To be sure, two of his covered foreign Internet contacts represent severed relationships that fall outside the parameters of the scope of question 9 and perforce his follow-up DSS interview and are perforce material to a Government investigation of the worthiness for a clearance candidate. The other three contacts covered in his signed, sworn statement and hearing testimony are significant and enduring enough to be classed as associates for purposes of question 9 and were clearly covered subjects in need of identifying. Applicant acknowledges as much, attributing his omissions to embarrassment, fears of being perceived as a "loser" and concerns over his being perceived as someone who was trying to hide something. So, as these contacts cross the threshold contact line for being considered associates, they warrant, too, the application of two of the disqualifying conditions for falsification: DC 2 (deliberate omission of falsification of a security form) and DC 3 (deliberately providing false or misleading information to an investigator).

Applicant, however, quickly realized his lack of complete candor about his foreign Internet contacts after adjourning his initial DSS interview and called the DSS agent back within minutes to complete the interview. In this second interview, he provided the full details of all of his foreign Internet contacts, including his since severed relationships. His disclosures satisfy the requirements of a prompt, good faith correction of a previous material omission. Applicant may take full advantage of MC 3 (prompt, good faith disclosure) of the Adjudicative Guidelines for personal conduct and in the process mitigates the adverse trustworthiness implications of his earlier omissions. Favorable conclusions warrant with respect to sub-paragraph 1.a of Guideline E.

In reaching my recommended decision, I have considered the evidence as a whole, including each of the E 2.2 factors enumerated in the Adjudicative Guidelines of the Directive.

FORMAL FINDINGS

In reviewing the allegations of the SOR and ensuing conclusions reached in the context of the FINDINGS OF FACT, CONCLUSIONS, CONDITIONS, and the conditions and factors listed above, I make the following FORMAL FINDINGS:

GUIDELINE E (PERSONAL CONDUCT): FOR APPLICANT

Sub-para. 1.a: FOR APPLICANT

Sub-para. 1.b: FOR APPLICANT

DECISION

In light of all the circumstances presented by the record in this case, it is clearly consistent with the national interest to grant or continue Applicant's security clearance.

Roger C. Wesley

Administrative Judge

1. ICQ is a popular method of Internet communication that provides instant messaging (ex. 3). ICQ permits a user to send a message that immediately pops up on an online screen known as a chat room. It lets the user chat, send e-mails, JMS, and wireless-pager messages (*see* ex. 3).