DATE: June 10, 2005

In Re:

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

Applicant for Security Clearance

ISCR Case No. 02-29244

DECISION OF ADMINISTRATIVE JUDGE

ELIZABETH M. MATCHINSKI

APPEARANCES

FOR GOVERNMENT

James B. Norman, Esq., Department Counsel

FOR APPLICANT

Pro Se

SYNOPSIS

Applicant misused a government information technology system by accessing the Internet for personal purposes, including adult (pornographic) sites at work on multiple occasions from about July 2001 to mid-October 2001. He was terminated from his defense contractor employment for cause in January 2002 as a result of his misconduct. His disregard of known regulations and policies regarding the use of a government-provided computer system raises serious concerns about his overall judgment, reliability, and trustworthiness, and his willingness and ability to properly protect classified systems, networks, and information. Clearance is denied.

STATEMENT OF THE CASE

On February 6, 2004, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) to the 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 the Applicant.[(1)] DOHA recommended referral to an administrative judge to determine whether his clearance should be granted, continued, denied, or revoked. The SOR was based on misuse of information technology systems (Guideline M) and personal conduct (Guideline E).

Applicant answered the SOR on March 17, 2004, contending that since a Letter of Consent had been issued June 6, 2003, granting him a secret-level security clearance, there was no basis to issue the SOR. He requested a hearing before a DOHA administrative judge if further processing was required. On July 19, 2004, the case was assigned to me and a hearing was scheduled for August 16, 2004. On July 24, 2004, Applicant moved for a 60-day continuance as he had not yet received his investigative file in response to his requests of February 25, 2004, and May 26, 2004, and because of work commitments that negatively impacted his ability to prepare and could preclude his availability on August 16, 2004. A continuance was granted and on August 5, 2004, the hearing was rescheduled for September 21, 2004.

At the hearing on September 21, 2004, six government exhibits and eight Applicant exhibits were entered into the record, exhibits 2, A, and B over objections. Applicant also testified, as reflected in a transcript received on October 4,

2004. The record was held open for two weeks for Applicant to rebut computer cookie logs included in government exhibit 2 and to prove defense contractor personnel were not notified of the military installation's prohibition against their using government-provided Internet access for personal use.

On October 5, 2004, Applicant forwarded a letter from a former coworker and he requested an extension to submit records of his frequent flyer miles with a U.S. carrier for 2000. Department Counsel having no objection thereto, the letter from the former coworker was admitted as exhibit I, and Applicant's correspondence to the airline as exhibit J. Applicant was granted an extension to November 2, 2004, to submit documentation of his airline travel.

On November 5, 2004, Applicant requested a further extension since the airline had not yet provided the travel documentation. During a conference call of November 8, 2004, Applicant was given a new deadline of December 6, 2004, to submit frequent flyer records or credit card records reflecting travel charged to his account, or both. On December 6, 2004, Applicant offered a redacted credit card statement with a closing date of October 11, 2000, to show he had been away from work the week of September 17, 2000. On December 8, 2004, the government objected, contending the document was irrelevant, lacked any probative value, and was incomplete. By order of December 13, 2004, Applicant was given until January 6, 2005, to respond to those concerns.

On January 7, 2005, Applicant timely forwarded an unredacted version of his credit card statement, and an affidavit from his spouse with a statement of her credit card account confirming his visit to her sometime during the week of September 20, 2000.[(2)] After consideration of the parties' respective positions, the unredacted credit card statement was admitted as Exhibit K on January 7, 2005, and the government was granted until January 14, 2005, to submit any objections to the affidavit of Applicant's spouse and statement of her credit card account. The government having no objection, those documents were marked and admitted as Exhibit L.

RULING ON PROCEDURE

In his Answer and at the hearing, Applicant challenged the government's authority to issue an SOR since a Letter of Consent had been issued in June 2003 granting him a secret clearance after the Defense Security Service (DSS) had completed its investigation of his misuse of government-provided Internet access and after his current employer had been notified that a decision had been made to grant Applicant a clearance. The government countered Applicant's secret-level security clearance had been reinstated to him as a routine, interim action since there had been less than a two-year break in service between Applicant's defense contractor employments, pending investigation and final adjudication of Applicant's security suitability. Based on the evidence adduced at the hearing, the salient jurisdictional facts are as follows:

On March 26, 1984, Applicant was hired as a computer systems analyst by a defense firm (company X) subcontracted to provide computer software development and testing services for the United States military. Applicant held a secret level security clearance for his work in electronic surveillance measures for the U.S. Air Force and had been stationed on the military installation full-time since the mid-1990s. Effective January 11, 2002, Applicant's access to government computers and networks was permanently revoked for unauthorized use of a government computer and government provided Internet access (viewed pornographic materials and other personal sites). On January 14, 2002, company X submitted an adverse information report as required by Section 1-302a of the National Industrial Security Operating Manual (NISPOM), notifying the Defense Security Service (DSS) that Applicant had "exercised unauthorized use of Government computer and internet." On January 25, 2002, Applicant was terminated for cause by company X because of his misuse of government-provided Internet access.

On March 11, 2002, Applicant began working as a software test engineer for his present employer (company Y). Company Y requested Applicant's secret-level clearance be continued. In about April 2002, the Defense Industrial Security Clearance Office (DISCO) notified company Y Applicant would not be granted a security clearance pending a full investigation into the incident that led to his termination from his previous job. In May and June 2002, the Defense Security Service conducted a personnel security investigation (standard expanded national agency check) of Applicant's security suitability, focusing on his misuse of the computer at the military installation in 2001. The investigation included an interview of Applicant. DSS closed its investigation on July 30, 2002, and referred the matter to DOHA on or about August 2, 2002.[(3)] Company Y was notified that Applicant's case had been submitted for adjudication. On June

6, 2003, DISCO issued a Letter of Consent, notifying defense contractor requestor company Y that Applicant had been granted a secret security clearance.[(4)] Applicant was then given access to classified information by his employer. On February 5, 2004, DOHA issued the SOR based solely on Applicant's misuse of a government computer and government-provided Internet access (viewed pornographic materials and other personal sites) while employed by company X.

Under Section 2-203 of the NISPOM, and ¶ C4.1.1. of Department of Defense Regulation 5200.2-R, *Personnel Security Program* (incorporated by reference in DoD Directive 5220.6), federal agencies that grant security clearances (top secret, secret, confidential, Q or L) to their employees or contractor employees must determine whether such employees have been previously cleared or investigated by the federal government. Any previously granted security clearance that is based on a current investigation of a scope that meets or exceeds that necessary for the clearance required, shall provide the basis for issuance of a new clearance without further investigation unless significant derogatory information that was not previously adjudicated becomes known to the granting agency, or there has been a break in military/federal employment of greater than 24 months (*see* 5220.2-R ¶ C4.1.3.1.). Applicant's use of government-provided computer Internet access to view pornography constituted significant new derogatory information that justified the DSS investigation in 2002. There is no evidence of any further investigation once the case was referred to DOHA. The salient issue here is whether the Letter of Consent represents a final favorable adjudication binding on DOHA, either under the reciprocity provisions of the NISPOM and 5200.2-R, or under general legal principles of collateral estoppel, equitable estoppel, or res judicata.

As a general matter, DOHA is bound by Section 2-203 of the NISPOM, and would be required to accept another agency's final adjudication. It is not clear whether the Letter of Consent was issued by DISCO on order of DOHA-Columbus or on its own initiative. However, once DISCO referred Applicant's case to DOHA for adjudication, the DoD Directive 5220.6 applies (*see* Directive 5220.6 ¶¶ 2.3. and E3.1.1.), and any unilateral decision by DISCO to adjudicate the matter favorably and issue the clearance would be ultra vires and not binding on DOHA. Assuming *arguendo* DOHA-Columbus had directed DISCO to grant the clearance, then the reciprocity provisions would in any event not apply. While it is vital that the adjudication decisions of DOHA be considered final by contractors, applicants, and even those other federal agencies with authority to grant clearances due to the reciprocity requirement, there is nothing in the NISPOM 5200.2-R, or Directive 5220.6 that would prohibit DOHA from issuing an SOR if the clearance was issued prematurely or inadvertently in error. As noted by the DOHA Appeal Board in ISCR Case No. 03-04172, decided June 7, 2005, the NISPOM's reciprocity provision does not preclude a federal agency from reevaluating whether a person should continue to retain a security clearance that was previously granted by that federal agency.[(5)]

FINDINGS OF FACT

DOHA alleged Applicant used a government computer and government-provided Internet access to view pornography and other personal sites while employed by a defense contractor, raising security concerns under Guideline M, misuse of information technology, and Guideline E, personal conduct. In his Answer, Applicant denied using a government computer. Applicant admitted he had misused government-provided Internet access to view pornography, but contested the revocation of his secret-level security clearance on that basis. After a thorough review of the evidence of record, I make the following findings of fact:

Applicant is a software test engineer for a defense contractor (company Y). Applicant, who worked for the company from June 1977 through March 1984, was rehired in March 2002 after he had been terminated from another defense contractor (company X) for cause in January 2002. Applicant seeks to retain a secret security clearance that was reinstated to him in June 2003.

In late March 1984, Applicant went to work for company X as a senior software engineer where he provided technical expertise in the areas of advanced warning radar software and software quality assurance. Due to his productivity and demonstrated willingness to assume a leadership role, Applicant was transferred to a newly created department in about November 1988 where he functioned as a software engineering manager with broader responsibilities, including the hiring and assignment of software personnel. Over the next year, he led the company's effort to work on a military program and earned very good ratings in all areas of his job performance. By November 1991, he was managing both a radar software quality assurance program for the military and a NATO software configuration project. "Top notch,

thorough and hard hitting," Applicant had established an excellent working relationship with his customers.

By 1995, Applicant's full-time duty station was at the customer site--a U.S. military base--where his employer was subcontracted to provide engineering and technical support. As a contractor on the military installation, Applicant was provided Internet access via the military computer network. His computer was purchased by his employer for another employee who had left the company. Under the Joint Ethics Regulation then in effect, the Internet was not to be used for any unofficial purpose. On February 20, 1996, the base commanding general issued a memorandum to all base members to stop Internet abuse. On March 25, 1996, the regulation was changed to permit government employees to use the Internet for unofficial purposes under certain circumstances (authorized by command, no adverse effect on performance of official duties, of reasonable duration and frequency, serve a legitimate military interest, no adverse impact on the military or DoD, no burden or significant expense to the military). On November 27, 1996, the base commander by memorandum for distribution authorized government employees to use the Internet for personal research or communications, subject to the specific limitations. Support personnel were notified they were not authorized to use government provided Internet access for personal use. Government and support personnel were notified that accessing pornographic material (graphics or text), forwarding chain letters, soliciting or selling (except on authorized bulletin boards establishing such use), violating any statute or regulation, mishandling classified information, and other uses incompatible with public service, were expressly prohibited. On logging on to the military network, computer users on the base, including the Applicant, were notified of the prohibited uses and had to assent to the policy before gaining access to the network.

Applicant continued to do an excellent job and was considered by his employer to be "a valued asset." In July 1995, he was appointed the base lead for a flight test program and co-chairman of a test plan working group. In August 1995, he was assigned lead software database responsibilities for a French software development and testing program, while continuing to support the advanced warning radar test and NATO electronic support measures programs. At Applicant's and his immediate supervisor's request, their military customer reviewed Applicant's qualifications and tasks to determine a proper categorization for him in light of his increased responsibilities and capabilities on behalf of the military. In early June 1997, Applicant's labor categorization was changed from journeyman scientist to engineering technician II--an elevation that his immediate supervisor felt was much deserved and overdue--with a $30,000 increase in Applicant's annual salary.

Applicant continued to successfully manage several critical functions supporting communication, navigation, computer and displays and international ITPs. With much of his work involving NATO, French, and United Kingdom programs, Applicant began to arrive early for work so that he could reach his customers during their normal working day. In June 1999, Applicant's superb software and test program analysis was formally recognized by his U.S. military customer. Throughout that year, Applicant was such a major contributor on the French electronic support measures program that the French military specifically requested his presence on a test team and his full support on the installation and testing on three remaining aircraft. In early 2000, it was proposed that he work in France for two to five years. While that job opportunity was under discussion, a new program manager was appointed by his U.S. military customer. The new program manager, a federal civilian, did not approve of the job transfer. Applicant believed he had been unfairly denied the opportunity by a program manager whom he perceived as not appreciative of his work and as threatening of his continued presence on the program.[(6)] Applicant complained of his frustrations to his immediate supervisor at company X to no avail.

On several occasions in 2000, Applicant accessed the Internet for personal reasons via the base's computer network. Applicant used a Gateway 2000 computer provided by the government.[(7)] Applicant knew contractors were prohibited from using the government-provided Internet for personal reasons, but the policy was not being strictly enforced. In about July 2001, he began viewing pornography via the Internet at work. While it began inadvertently by clicking on a neutrally named site that turned out to be a pornographic website, by September 2001 he was intentionally viewing pornography. Well aware of the policy that expressly prohibited all base personnel from accessing pornography at work, Applicant continued his viewing of pornography through government-provided Internet access after September 11, 2001. He also accessed websites that did not contain pornography, including retail and financial web addresses, but were unrelated to his official duties.

Following the terrorism act of September 11, 2001, the base was closed to nonessential personnel for a few days. Not

ordered to report to work until the following Monday, September 17, 2001, Applicant traveled out of state to see his girlfriend (now spouse) and was away from his work on at least September 20, 2001.

Applicant's illegal access was subsequently detected through computer network monitoring at the base. On October 30, 2001, Applicant's computer was seized and he was interviewed by a security forces investigator about his alleged illegal use of a government computer and access to pornography. Applicant provided a statement in which he admitted using his computer and government-provided Internet access for personal tasks after he had completed his work assignments:

While some of this included looking at sites that had news, financial information, sports, etc., there were times when curiosity and boredom would lead me to look at sites such as personal ads which sometimes lead to content and pictures of adult nature. Also, sometimes using search engines to find one type of item (such as friends) would lead to sites having adult content. Curiosity would lead me to sometimes viewing adult material and pictures.[(8)]

Applicant expressed remorse for the mistakes he had made and expressed his desire to remain in his position at the base. In response to specific questions from the investigator, Applicant indicated his access to pornography began approximately six months earlier. Computer forensic media analysis of two squid proxy server logs revealed Applicant had accessed 18 + sexually explicit adult sites and 30+ sexually explicit adult images from October 17, 2001 through October 26, 2001. The tracking record reflected Applicant had spent as long as 45 minutes on one of the pornographic websites. He had also downloaded numerous sexually explicit pictures.

At the referral of company X's employee assistance program, Applicant met with a counselor twice in November 2001. Applicant exhibited emotional distress and self doubt caused by his frustrations and disappointment with the loss of the work project in France and exacerbated by the personal loss of two friends in the terrorist acts of September 11. In the opinion of the counselor, he turned to accessing adult websites at work to seek diversion and relief, but was on the way to restoring his emotional balance when she last met with him.

Applicant was led to believe by both the U.S. military as well as his employer that his misconduct was a serious violation, but he would not face adverse action because of his otherwise excellent work record. Well liked by the French, Applicant was considered indispensable. His performance rating of November 2001 reflects he was considered a top performer with enthusiasm, technical competence and initiative. Concerning Applicant's recent use of the government-provided Internet to view inappropriate adult material, it was remarked that both the government customer and the company regarded it as a "first time violation of rules of an otherwise excellent employee who has consistently been a superior performer over the years."

On or about December 14, 2001, the military contracting officer for the advanced warning radar program first learned that Applicant had accessed pornography at work in October. After consulting with legal personnel at the base, the contracting officer revoked permission for Applicant to use government computers and networks as of January 11, 2002, for violating Joint Ethics Regulation (DoD 5500.7-R) and the base's policy for Internet use (storing or displaying obscene material is not authorized and support contractor personnel are not authorized to use government-provided Internet access for personal use). Company X was notified that $718.65 would be deducted from its next monthly invoice to recover money for the time Applicant used the base network for personal purposes. Since Applicant could not perform his job without access to the network, the military requested Applicant be removed from the project. On January 25, 2002, Applicant was involuntarily terminated by company X for cause (misuse of the government computer and Internet).

He is not eligible to be rehired.

Applicant was interviewed by a Defense Security Service special agent on June 5, 2002, about his improper computer access at work in 2001. Applicant admitted he knew military policy prohibited contractors from having access to the Internet for personal use and that access to pornographic sites was strictly prohibited. When he accessed the military base's computer network a warning appeared informing him that personal access was prohibited, but he indicated the policy was not being enforced. Applicant attributed his misuse of computer access to his frustrations with the program manager, who he claimed deliberately excluded him from meetings he should have attended. Applicant acknowledged he had made a mistake but he felt his employment termination was "an overly severe consequence" and others were

doing it.

In March 2003, Applicant returned to work for company Y after almost 19 years at company X. On his job application, Applicant listed his employment with company X but gave no reason for leaving the job. He also requested that company Y not contact company X as he wanted to start work there "with a clean slate." Applicant's performance over the March 2003 to February 2004 ratings period met his lead and management's expectations.

Applicant has been involved in performance dance in his area since at least 1984. He serves on the Board of Directors of a nonprofit camp operating traditional music and dance programs for adults.

POLICIES

"[N]o one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988). As Commander in Chief, the President has "the authority to . . . control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to occupy a position . . . that will give that person access to such information." *Id.* at 527. The President has authorized the Secretary of Defense or his designee to grant applicants eligibility for access to classified information "only upon a finding that it is clearly consistent with the national interest to do so." Exec. Or. 10865, *Safeguarding Classified Information within Industry* § 2 (Feb. 20, 1960). Eligibility for a security clearance is predicated upon the applicant meeting the security guidelines contained in the Directive. An applicant "has the ultimate burden of demonstrating that it is clearly consistent with the national interest to grant or continue his security clearance." ISCR Case No. 01-20700 at 3.

Enclosure 2 of the Directive sets forth personnel security guidelines, as well as the disqualifying conditions (DC) and mitigating conditions (MC) under each guideline. In evaluating the security worthiness of an applicant, the administrative judge must also assess the adjudicative process factors listed in ¶ 6.3 of the Directive. The decision to deny an individual a security clearance is not necessarily a determination as to the loyalty of the applicant. *See* Exec. Or. 10865 § 7. It is merely an indication that the applicant has not met the strict guidelines the President and the Secretary of Defense have established for issuing a clearance.

Concerning the evidence as a whole, the following adjudicative guidelines are most pertinent to this case:

Misuse of Information Technology Systems. Noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual's trustworthiness, willingness, and ability to properly protect classified systems, networks, and information. Information Technology Systems include all related equipment used for the communication, transmission, processing, manipulation, and storage of classified or sensitive information. (E2.A13.1.1.)

Personal Conduct. 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. (E2.A5.1.1.)

CONCLUSIONS

Having considered the evidence of record in light of the appropriate legal precepts and factors, I conclude the government established its case with respect to Guideline M, misuse of information technology systems, and Guideline E, personal conduct. Applicant knowingly violated his military customer's policies regarding the use of government computers and government-provided Internet service in 2000 and 2001. Cookie logs of record reflect access through Applicant's work computer of several websites unlikely to have any reasonable application to official duties on behalf of the U.S. military. Applicant challenges the validity of the cookie logs, which contain entries for September 14, 18, 19, 20, and 21, 2001, based on the closure of the base to him after September 11, 2001 until September 17, 2001, and he was out of the area visiting his girlfriend the week of September 17, 2001. Applicant presented corroboration only for his absence from work on September 20, 2001. Assuming he was out of work through September 21, 2001, it would indicate only that he did not use his work computer on those dates, and would not invalidate the entire cookie logs.

Applicant has not questioned the computer forensic media analysis that revealed he accessed through his work computer

18 + sexually explicit adult sites and 30 adult images between October 17, 2001 and October 26, 2001. He has admitted visiting personal websites via government-provided Internet access--including pornography starting in July 2001--despite being reminded of the prohibitions against personal use by contractors every time he logged on. Under Guideline M, misuse of information technology, disqualifying conditions E2.A13.1.2.1. *Illegal or unauthorized entry into any information technology system*, E2.A13.1.2.3. *Removal (or use) of hardware, software or media from any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations*, and 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*, apply. There is no question that access to, and downloading of, pornography through a government computer and government-provided Internet access are strictly prohibited by regulation and base policy. Pertinent disqualifying conditions under Guideline E, personal conduct, are E2.A5.1.2.1. *Reliable, unfavorable information provided by associates, employers, coworkers, neighbors and other acquaintances*, E2.A5.1.2.4. *Personal conduct or concealment of information that increases an individual's vulnerability to coercion, exploitation or duress, such as engaging in activities which, if known, may affect the person's personal, professional, or community standing or render the person subject to blackmail*, and 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*.

The misuse of information technology equipment used for the communication, transmission, processing, manipulation, or storage of classified or sensitive information, may be mitigated where the misuse was not recent or significant (E2.A13.1.3.1.), the conduct was unintentional or inadvertent (E2.A13.1.3.2.), the introduction or removal of media was authorized (E2.A13.1.3.3.), the misuse was an isolated event (E2.A13.1.3.4.), or the misuse was followed by a prompt, good faith effort to correct the situation (E2.A13.1.3.5.). There is no evidence Applicant has improperly accessed a computer or computer network at his current employment. While his misuse of the computer and Internet access is not recent, it cannot reasonably be termed insignificant. Moreover, it was intentional and repeated. Applicant's inappropriate access continued until he was caught through computer monitoring. Although he is credited with acknowledging when confronted that he had accessed adult sites, this is not enough to apply E2.A13.1.3.5. Similarly, none of the mitigating conditions under Guideline E apply in his favor. Although his former coworkers know of his access to pornography, Applicant did not inform his current employer of the circumstances that led to his discharge from company X and he did not authorize company Y to contact company X. He has not taken sufficient steps to reduce his vulnerability to coercion, exploitation, or duress.

Applicant's failure to satisfy the mitigating conditions set forth in the Directive does not necessarily mandate an adverse outcome. Under the "whole person" concept, an applicant is to be judged by the totality of his acts and omissions. It requires the careful weighing of a number of factors, including the nature, extent and seriousness of the conduct (E2.2.1.1.), the circumstances such as knowledgeable participation (E2.2.1.2.), frequency and recency (E2.2.1.3.), the individual's age and maturity (E2.2.1.4.), voluntariness of participation (E2.2.1.5.), the presence or absence of rehabilitation (E2.2.1.6.), motivation (E2.2.1.7.), the potential for pressure, coercion, exploitation, or duress (E2.2.1.8.), and the likelihood of continuation or recurrence (E2.2.1.9.). Especially given his maturity and job experience, his intentional disregard of the base's computer use policies raises serious doubts for his judgment, reliability, trustworthiness, and willingness to adhere to rules and regulations. Not all of his unauthorized access can be attributed to the stress of September 11, 2001, as his viewing of pornography and other personal websites began months before the terrorism. Deliberate violations cannot be justified on the basis of personal frustration with a program manager, the loss of a deserved assignment (Tr. 124-25), or that the policy prohibiting personal use by contractors was not being followed by other personnel or enforced.

To his credit, Applicant contacted company X's employee assistance program after his misuse of the computer was discovered, and he had two sessions with a counselor in an effort to understand why he accessed pornography. While he has apologized, he continues to minimize his misconduct ("the incident was minimal . . . most of the sites that were accessed were of less than ten seconds." Tr. 76) and assigns blame to others, such as the military who he maintains did not follow its own policy on corrective actions to be taken in cases of extended or repeated visits by a user to the same adult website or downloading of pornographic material from the Internet. (Tr. 72) Applicant's contributions to the defense effort are well documented and significant, but they did not deter him from misusing the base's information technology system. Applicant having failed to meet his heavy burden of overcoming the security concerns engendered by his misuse of information technology systems, I find against him as to ¶¶ 1.a. and 2.a. of the SOR.

FORMAL FINDINGS

Formal Findings as required by Section 3. Paragraph 7 of Enclosure 1 to the Directive are hereby rendered as follows:

Paragraph 1. Guideline M: AGAINST THE APPLICANT

Subparagraph 1.a.: Against the Applicant

Paragraph 2. Guideline E: AGAINST THE APPLICANT

Subparagraph 2.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 Applicant. Clearance is denied.

Elizabeth M. Matchinski

Administrative Judge

1. The SOR was issued under the authority of Executive Order 10865 (as amended by Executive Orders 10909, 11328, and 12829) and Department of Defense Directive 5220.6 (Directive), dated January 2, 1992 (as amended by Change 4).

2. Applicant encountered facsimile transmission problems on January 6, 2005, not of his own making, so the documentation received on January 7, 2005, was considered timely.

3. The DSS investigative report entered as Exhibit A reflects DOHA-Columbus involvement as of August 2, 2002. Pursuant to ¶ E3.1.1. of Department of Defense Directive 5220.6, DISCO is to make a referral to DOHA (and DOHA thereby is given jurisdiction) when it cannot affirmatively find that it is clearly consistent with the national interest to grant or continue a security clearance for an applicant.

4. The Letter of Consent is not of record, although Applicant's performance evaluation for the period March 2003 to February 2004 indicates he received his secret clearance. (Ex. E) Applicant indicated the grant of clearance was based on a favorable NAC of June 29, 1995. A grant of clearance solely based on that dated NAC would be in violation of DoD 5200.2-R, ¶ C3.4.1.2. Under that provision, a final or interim personnel security clearance may be granted only if the investigative requirements are complied with, all available information has been adjudicated, and a finding made that such clearance would be clearly consistent with the interests of national security. Pertinent regulations would require consideration of the security implications of Applicant's viewing of pornography using government-provided Internet access before he could be granted his final secret clearance. As noted by the DOHA Appeal Board in ISCR Case No. 03-04172 (June 7, 2005), under Section 2-203 of the NISPOM, "reciprocity is predicated on: (a) a person having an existing security clearance, (b) based on a current investigation, (c) of a scope that meets or exceeds that necessary for the security clearance at issue, and (d) the absence of significant derogatory information that was not previously adjudicated."

5. This affirms an earlier Board ruling in ISCR Case No. 99-0454, decided October 17, 2000, that the obligation of reciprocity to security clearance decisions made by other federal agencies does not limit or control the authority of a federal agency to reopen or reconsider its own decisions.

6. Applicant took statements from the program manager such as "I'm not sure there is very much work in this area left to do" as indications that the program manager wanted him removed from the program. Applicant also felt the program manager had embarrassed him intentionally at social events. (Ex. 5) Yet, when interviewed by the Defense Security Service, this program manager related Applicant was very competent and he recommended Applicant for a security clearance. (Ex. A) Applicant's immediate supervisor at company X from 1991 to October 2001 expressed his belief the job opportunity in France failed to materialize for Applicant because the prime contractor on the project felt its team

was more than adequate to handle the work in France. The record does not support Applicant's claims that the government program manager was intentionally thwarting his professional growth.

7. Applicant's permission to use government computers and networks was revoked by the U.S. military for illegal use of a government computer as well as unauthorized use of government provided Internet access. (Ex. 1) Applicant failed to prove that the computer was provided instead by his employer. He presented only a memorandum concerning a request for salary increase in 1998 wherein he indicated he had up-to-date computer equipment that had been purchased by company X for another employee. The computer seized in October 2001 was a Gateway 2000. (Ex.1) Company X's human resources director indicated Applicant admitted to him that he had accessed pornographic sites using the government computer. (Ex. A)

8. While it is not doubted that Applicant experienced emotional distress, especially after the terrorist act of September 11, 2001, curiosity played a large part in his viewing of pornography and in his return to some adult sites.