DATE: December 2, 2004

In Re:

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

Applicant for Security Clearance

ISCR Case No. 03-08175

ECISION OF ADMINISTRATIVE JUDGE

JOSEPH TESTAN

APPEARANCES

FOR GOVERNMENT

Jennifer I. Campbell, Department Counsel

FOR APPLICANT

Eric Chase, Esq.

SYNOPSIS

Applicant's use of government computers to access and download sexually explicit images, including child pornography, on a frequent basis over a long period, in knowing violation of agency regulations, reflects adversely on his judgment. Clearance is denied.

STATEMENT OF THE CASE

On March 3, 2004, 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 denied or revoked.

Applicant responded to the SOR in writing on March 31, 2004. The case was assigned to the undersigned on June 9, 2004. A Notice of Hearing was issued on July 19, 2004 setting the hearing for August 12, 2004. Applicant requested a continuance, which was granted. An Amended Notice of Hearing was issued on August 4, 2004, and the hearing was held on August 26, 2004. The transcript was received on September 13, 2004.

FINDINGS OF FACT

Applicant is a 49 year old engineer. He has worked for his current employer for over four years. Exhibits A, B and C establish that applicant performs well for his current employer.

While working at a prestigious government agency as a Group Supervisor, applicant developed a software application that, in essence, scanned the Internet for pornographic images. Applicant would launch this application after logging onto his government work station computer,[(1)] and while he was performing his regular duties, the application searched

the Internet for pornographic images. After a period of time applicant would check the status of the search, and if it had finished, he would either download the pornographic images onto his government work station computer and then transfer them to his own personal computer, or he would delete the images.[(2)] Applicant engaged in this activity on a frequent basis over a long period of time.

Based on the evidence presented, I find that applicant did not intentionally seek out child pornography. However, after using his application for many years, it became obvious to him that among the thousands of pornographic images he would regularly access and download to his government work station computer, a small percentage of the images constituted child pornography. Applicant handled the child pornography "problem" by deleting these images when he came across them. His application had no way of differentiating pornography from child pornography, and applicant never attempted to change the application to filter out child pornography (TR at 124).

In 1994, applicant used his government work station computer to post pornographic material on an off site location. Someone complained to one of applicant's colleagues, who informally advised applicant that posting such material was against agency policy and he should stop this activity. Applicant protested to the colleague that his free speech rights gave him the right to post what he wanted. Although applicant did not tell the colleague he would stop, applicant appears to have stopped posting pornography from his government work station computer at that time (Exhibit 14; TR at 109).

Also in 1994, the Deputy Director of applicant's agency issued a memorandum that explicitly stated agency policy prohibited accessing inappropriate material, such as sexually explicit pictures, on government time or by using government property (Exhibit 42). Applicant testified that he never saw this memo (TR at 104).

In 1998, applicant attended an ethics briefing where he was informed that it was his agency's policy that government work station computers could not be used to access or download pornography, and that violation of the policy could result in disciplinary action, up to and including dismissal. Despite this admonition, applicant continued to access and download pornography onto his government work station computer. Applicant testified that he continued the prohibited activity because he felt his employer (1) was not serious about the policy and (2) was being hypocritical by prohibiting him from accessing and downloading pornography onto his work station computer while at the same time providing agency employees access to an onsite agency server which held the same pornographic images. In his view, he had the right to access anything that was on the agency's server, regardless of ethics guidelines to the contrary. Applicant continues to believe this (TR at 136-137, 144-145).

An investigation of applicant was initiated in early 1998 after his agency's Inspector General was notified by a police department in another state that child pornography had been found on a server that had been traced back to applicant's agency, and eventually to applicant. The investigation, which lasted over a year, resulted in a finding that applicant accessed and downloaded sexually explicit images in violation of several agency policies and guidelines, and eventually resulted in applicant's "resignation in lieu of termination for cause" (Exhibit 40).[(3)]

Applicant's case was referred to the U.S. Attorney's office for possible prosecution under the child pornography laws. The U.S. Attorney declined to prosecute applicant because applicant did not transmit the child pornography, and the number of images in applicant's possession was considered minimal. There is conflicting evidence in the record concerning whether State misdemeanor charges were filed against applicant. However, even if such charges were originally filed, they were not pursued because the one year statute of limitations on such charges had expired (Exhibit 38).

In September 2000, applicant gave a signed, sworn statement to the Defense Security Service (DSS). In it, he stated that he had denied to his former agency's investigators that he had downloaded child pornography onto his government work station computer. He further stated that, although he had admitted downloading sexually explicit images to that computer, these images were

all of an adult nature where the models were, to the best of his knowledge, at least 18 years old (Exhibit 40). Neither of these statements was true.[(4)]

In a signed, sworn statement he gave to DSS in July 2002, applicant stated, among other things, that since his termination in 1999, he has not used any of his employer's computers to access pornographic sites. He further stated he last visited a pornographic site (from his home computer) "probably at least six months ago" (Exhibit 39).

CONCLUSIONS

The evidence establishes that while employed at a Government agency in the 1990s, applicant knowingly violated agency regulations by accessing and downloading sexually explicit images onto his government work station computer on many occasions over a long period of time. The evidence further establishes that during the same time period, applicant knowingly accessed and downloaded child pornography onto the same computer in violation of 18 U.S.C. 2252.[(5)] The evidence further establishes that following an agency investigation, applicant was given the choice of being dismissed for cause (in which case he would have a right to appeal the dismissal) or resigning in lieu of being dismissed, and he chose the latter. Applicant's conduct reflects adversely on his judgment, reliability and trustworthiness, and strongly suggests he cannot be relied upon to safeguard classified information.

With respect to Guideline M, applicant's use of his government work station computer to access and download sexually explicit images, in violation of his agency's rules, regulations, guidelines, procedures and/or policies, requires application of Disqualifying Condition (DC) 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)*. The fact that applicant knowingly engaged in this activity on a frequent basis over a long period of time, and continued to engage in it after he was advised that it violated agency guidelines and could result in his dismissal, precludes application of any Mitigating Conditions (MC).

With respect to Guideline D, applicant's accessing and downloading of child pornography requires application of DC E2.A4.1.2.1 *(sexual behavior of a criminal nature, whether or not the individual has been prosecuted)*. Applicant's accessing and downloading sexually explicit images (including child pornography), particularly after he was advised that such activity could lead to his dismissal, requires application of DC E2.A4.1.2.3 *(sexual behavior that causes an individual to be vulnerable to coercion, exploitation, or duress)*, and DC E2.A4.1.2.4 *(sexual behavior of a public nature and/or that which reflects lack of discretion or judgment).* No MCs are applicable. MC E2.A4.1.3.2. is not applicable because there is evidence that applicant continued to access and/or download child pornography, albeit from his home computer, subsequent to his resignation from the government agency. MC E2.A4.1.3.3. is not applicable because there is other evidence of questionable judgment; namely, his continuing belief that he was entitled to use his government work station computer to access anything that was on the agency's server, regardless of what agency guidelines proscribed.

With respect to Guideline J, DC E2.A10.1.2.1 *(allegations or admission of criminal conduct, regardless of whether the person was formally charged*) is applicable because, as noted above, applicant's accessing and downloading of child pornography was criminal. Applicant has not met his burden in proving that any of the MCs under Guideline J are applicable.

With respect to Guideline E, the evidence does not establish that applicant continued to post pornographic material to offsite computers after he was advised by a colleague to cease this activity. Therefore, SOR Allegation 4.a. is found for applicant. However, using his work station computer to access and download sexually explicit material, including child pornography, requires application of DC E2.A5.1.2.4 *(personal conduct . . . 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 susceptible to blackmail)* and DC 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)*. Applicant's continuation of this activity after the 1998 ethics briefing is particularly troubling. No MCs are applicable.

There is a clear nexus between the improper and criminal conduct which led to applicant's resignation (particularly his knowing and wilful disregard of agency regulations), and his ability and/or willingness to safeguard classified information. Although it has been over four years since he engaged in the conduct that led to his resignation, the fact he continues to visit the same pornographic sites leads me to conclude that, despite applicant's superior intelligence, and all

he has gone through, he still does not appreciate the significance and magnitude of his misconduct.[(6)] Doubts about his judgment continue to exist, and these doubts must be resolved against him.

FORMAL FINDINGS

PARAGRAPH 1: AGAINST THE APPLICANT

PARAGRAPH 2: AGAINST THE APPLICANT

PARAGRAPH 3: AGAINST THE APPLICANT

PARAGRAPH 4: 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.

Joseph Testan

Administrative Judge

1. Applicant had installed his application on his employer's server and two other servers operated by private Internet companies with whom applicant had private accounts. By doing so, applicant was able to log onto his government computer and launch his application on any of the three servers. The pornographic images, obtained from any of the three servers, would then download onto his government work station computer.

2. If applicant wanted to keep the downloaded images he would transfer them from his government work station computer to his privately purchased media using a government provided zip drive.

3. Applicant's current employer is not aware of the reason for his departure from this job. His family is aware of the reason.

4. *See,* TR at 69, 98-99, 124-125; Exhibit 39.

5. As noted in the Findings of Fact, applicant did not intentionally seek out the child pornography. This fact, however, is irrelevant in determining whether applicant's conduct was criminal. Applicant clearly knew that his software application was accessing and retrieving child pornography. The fact that he continued to utilize his application with this knowledge is sufficient to satisfy the scienter requirement of 18 U.S.C. 2252.

6. In particular, applicant does not seem to understand that, although the U.S. Attorney declined to prosecute him, he could have been prosecuted for violating 18 U.S.C. 2252, and could have served a lengthy prison sentence if he were convicted.