KEYWORD: Information Technology; Personal Conduct

DIGEST: Applicant's improper use of his company computer to access pornographic sites for a four month period between January and May 2003, in violation of company policy, remains a security concern under the misuse of technology systems guideline and the personal conduct guideline. Clearance is denied.

CASENO: 03-25495.h1

DATE: 06/29/2005

DATE: June 29, 2005

In Re:

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

Applicant for Security Clearance

ISCR Case No. 03-25495

DECISION OF ADMINISTRATIVE JUDGE

PAUL J. MASON

APPEARANCES

FOR GOVERNMENT

Francisco J. Mendez, Jr., Esq., Department Counsel

FOR APPLICANT

Pro Se

SYNOPSIS

Applicant's improper use of his company computer to access pornographic sites for a four month period between January and May 2003, in violation of company policy, remains a security concern under the misuse of technology systems guideline and the personal conduct guideline. Clearance is denied.

STATEMENT OF CASE

On July 20, 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, amended April 4, 1999, issued a Statement of Reasons (SOR) to Applicant. The SOR detailed reasons under Guideline E (personal conduct) and Guideline M (misuse of information technology systems) 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 furnished his answer to the SOR on August 10, 2004. Applicant elected to have his case decided on a written record. The Government provided Applicant a copy of the File of Relevant Material (FORM) on August 25, 2004. Applicant received the FORM on August 31, 2004. His response to the FORM was due by September 30, 2004. No response was received. The case was assigned to me on November 1, 2004.

FINDINGS OF FACT

Applicant admitted both allegations of the SOR. His admissions shall be incorporated by reference in the following factual findings. Applicant is 47 years old and has been employed as a network technician for a defense contractor since 1985. He seeks a secret clearance.

As a network technician, Applicant does network installations at his company. From January to May 2003, Applicant's access time on the internet was about one or two hours a day depending on his workload. Applicant accessed inappropriate pornographic websites three times a week, up to 30 minutes on each occasion[(1)] from his company computer at his place of employment. He never viewed any child pornography. He knowingly violated his company's policy by inappropriately accessing the internet on his company computer to view pornographic sites. He was also aware that company computer security monitored inappropriate internet access.

In June 2003, Applicant was confronted by a company investigator and admitted his transgressions. Applicant explained his conduct began with suggestions by coworkers to view a website containing humorous content. From this website, Applicant's viewing expanded to pornographic sites. He rationalized his access time as minor because he always completed his assigned duties beforehand. Applicant's company imposed a 30-day suspension from work without pay.

In his sworn statement dated October 20, 2003, Applicant claimed he never downloaded, saved, or e-mailed pictures from these pornographic sites. He stressed he never accessed these sites on his home computer. He stated he never accessed another employee's computer for illicit purposes, and never engaged in any illegal entry of technology systems, and never tried to alter any part or procedure connected to a technology system, and never tried to introduce a virus into a technology system. Applicant also maintained he never tried to acquire or misuse encryption software. Applicant had never heard of any incidents involving the illegal transfer of United States technology.

Applicant points out that the "downtime" occasions have been resolved by his employer increasing the workload and raising the work output. Finally, he asserts he has no interest in viewing these sites because the incident is behind him.

POLICIES

Enclosure 2 of the Directive sets forth guideline conditions which must be given binding consideration in making security clearance decisions. These conditions must be considered in every case according to the pertinent guideline; however, the conditions are in no way automatically determinative of the decision in any case nor can they supersede the Administrative Judge's reliance on his own common sense.

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 and willingness to protect classified information.

Personal Conduct

Unwillingness to comply with rules and regulations could indicate the person may not properly safeguard classified information.

Burden of Proof

The Government has the burden of proving controverted facts by substantial evidence. After the Government meets its burden, an applicant has the ultimate burden of presenting evidence in refutation, extenuation, or mitigation that demonstrates it is clearly consistent with the national interest to grant or continue a security clearance. Any doubt concerning an applicant's security clearance should be resolved in favor of national security. *Department of the Navy v. Egan*, 484 U.S. 518, at 531.

CONCLUSIONS

The Government has established by substantial evidence and Applicant's admissions that he used his company computer to inappropriately access pornographic websites from January to May 2003. The frequency of his access to these sites was about three times a week. He spent up to 30 minutes in the sites each time he acquired access. Applicant's misuse of information technology systems (Guideline M) falls within disqualifying condition (DC) 1 E2.A1.3.1.2.1. (*illegal or*

unauthorized entry into any information technology system) and DC 3 E2.A13.1.2.3. (*removal (or use) of hardware, software or media from information technology system without authorization, when specifically prohibited by rules, guidelines or regulations*.) Applicant knew it was against company policy to access the internet to view pornographic material. Applicant also knew the company computer security system had devices to detect inappropriate access of the internet on company computers. In sum, Applicant's unauthorized entry into company computers (DC 1) was prohibited by company rules. (DC 3)

There are four mitigating conditions (MC) under the guideline that have potential application to the circumstances of this case. MC 1 E2.A13.1.3.1. (*the misuse was not recent or significant*) does not apply in this case as the conduct was within the last two years. In addition, the conduct was significant in that Applicant engaged in the proscribed activity for more than four months or about 12 times a month for up to 30 minutes per viewing occasion. MC 2 E2.A13.1.3.2. (*the conduct was unintentional or inadvertent*) will mitigate activity that is not intentionally carried out. MC 2 does not apply due to Applicant's deliberate behavior over a four month period. MC 3 E2.A13.1.1.3.3. (*the introduction of or removal of media was authorized*) does not apply to these facts. MC 4 E2.A13.1.3.4. *(the misuse was an isolated event*) addresses behavior that occurs only a few times. The facts of this case indicate Applicant viewed pornographic sites on at least 40 occasions within a four month period, and there is no indication he would have terminated his habit had he not been confronted by the company investigator in June 2003. Neither the company policy prohibiting access to pornographic sites nor the computer security surveillance system deterred Applicant from repeatedly accessing the sites. I find against Applicant under misuse of information technology systems (Guideline M).

Applicant's violation of the company policy also constitutes personal conduct (PC) within Guideline E. PC DC 5 E2.A5.1.2.5. (*a pattern of dishonesty or rule violations*) applies to the facts of this case because Applicant repeatedly violated his employer's policy forbidding inappropriate access of pornographic web sites on his employer's computer. While Applicant indicated he never abused or misused or otherwise harmed a technology system in any manner, the pivotal question remains how he was able to stop accessing the pornographic sites so abruptly after defying two pornographic policy prohibitions for four months. issing from Applicant's case in mitigation is evidence substantiating his claim he lost interest in these sites and how he was able to put the activity behind him. Applicant has mentioned lessons he has learned but has not discussed what those lessons were. Information related to the foregoing issues would allow me to assess the seriousness of Applicant's resolve to forego this pornographic activity in the future. An applicant has the ultimate burden of persuasion to show he has mitigated past inappropriate conduct and he warrants access to classified information. Applicant has not met his burden under the specific guidelines or the general policy factors of the whole person concept.

FORMAL FINDINGS

Paragraph 1. Guideline M (misuse of information technology systems): AGAINST THE APPLICANT.

a. Against the Applicant.

Paragraph 2. Guideline E (personal conduct): AGAINST THE APPLICANT.

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 Applicant a security clearance.

Paul J. Mason

Administrative Judge

1. Applicant described the time which he accessed the internet as "downtime on the job."