KEYWORD: Information Technology; Personal Conduct; Sexual Behavior

DIGEST: Applicant is 43 years old, married with two children, a military retiree, and works for a defense contractor. In 2003, he accessed pornographic web sites on his government information system computer for a six-month period during work hours. Applicant mitigated the misuse of information technology systems, personal conduct, and sexual behavior security concerns. Clearance is granted.

CASENO: 03-21853.h1

DATE: 02/13/2006

DATE: February 13, 2006

In re:

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

Applicant for Security Clearance

ISCR Case No. 03-21853

DECISION OF ADMINISTRATIVE JUDGE

PHILIP S. HOWE

APPEARANCES

FOR GOVERNMENT

Julie R. Edmunds, Esq., Department Counsel

FOR APPLICANT

Pro Se

SYNOPSIS

Applicant is 43 years old, married with two children, a military retiree, and works for a defense contractor. In 2003, he accessed pornographic web sites on his government information system computer for a six-month period during work hours. Applicant mitigated the misuse of information technology systems, personal conduct, and sexual behavior security concerns. Clearance is granted.

STATEMENT OF THE CASE

The Defense Office of Hearings and Appeals (DOHA) declined to grant or continue a security clearance for Applicant. On July 21, 2005, DOHA issued a Statement of Reasons[(1)] (SOR) detailing the basis for its decision-security concerns raised under Guideline M (Misuse of Information Technology Systems), Guideline E (Personal Conduct), and Guideline D (Sexual Behavior) of the Directive. Applicant answered the SOR in writing on August 8, 2005. Applicant requested his case be decided on the written record in lieu of a hearing.

On September 27, 2005, Department Counsel submitted the Department's written case, which included an amendment to subparagraph 1.b. about Applicant being given an opportunity to submit his resignation or be terminated by his employer after being removed from contract work for the White House Communications Agency (WHCA) as a result of using government computer equipment for purposes other than intended or allowed as set forth in subparagraph 1.a. of the SOR. A complete copy of the file of relevant material (FORM) was provided to the Applicant. He was given the opportunity to file objections and submit material in refutation, extenuation, or mitigation. Applicant filed a response to the FORM on October 24, 2005. The case was assigned to me on November 7, 2005.

FINDINGS OF FACT

Applicant's admissions to the SOR allegations are incorporated here as findings of fact. After a complete and thorough review of the evidence in the record, and full consideration of that evidence, I make the following additional findings of fact:

Applicant is 42 years old, married with two children, and works for a defense contractor. He is a military retiree with 20 years of service. (Items 4 and 6)

Applicant worked for a defense contractor who provided information technology services for the WHCA from March 2003 to December 2003. Applicant used the government computer workstation from June 2003 to December 2003 to view pornographic web sites during work hours. His employer discovered it while performing a routine security review. On December 16, 2003, his employer confronted Applicant with the information concerning his use of he government computer system to view pornography. His employer had 100 pages of printable pornographic material from Applicant's computer. His employer gave him a chance to explain his conduct. Applicant eventually admitted the misuse of his government computer equipment, in violation of DoD Directive 5500.7-R, Section 2-301.a.2.d. prohibiting the use of Federal Government communications systems to any use involving pornography. Disciplinary action started, and on December 18, 2003, Applicant resigned his position with his employer. His employer gave him the choice of being terminated or resigning. His employer did attempt to find him work within the company that did not require working on the WHCA, but could find any work within it because all employees are direct charges on contracts in the low overhead company. Within this context Applicant decided to resign. (Items 3 and 5, FORM Response)

Applicant applied for new employment with another contractor on or about January 15, 2004. He has worked for that employer since then. Applicant's current employer is pleased with his duty performance, with a company vice president stating of the six trainers in the training group, Applicant "is constantly singled out as the very best". Applicant has been given the Contractor of the Quarter award twice since he started working for his present employer in February 2004. He was nominated a third time in late 2005 for the same award. His employer states his duty performance is exceptional and there are no client complaints about Applicant. His project manager trusts him and has confidence in him. His former employer also thought highly of his work product, but had no other job positions for him when he was removed from his WHCA position at the request of that agency. (FORM Response)

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 the national interest to do so." Exec. Or. 10865, *Safeguarding Classified Information with 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.

The adjudication process is based on the whole person concept. All available, reliable information about the person, past and present, is to be taken into account in reaching a decision as to whether a person is an acceptable security risk. Enclosure 2 of the Directive sets forth personnel security guidelines, as well as the disqualifying conditions (DC) and mitigating conditions (MC) under each guideline that must be carefully considered in making the overall common sense determination required.

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. Those assessments include: (1) the nature, extent, and seriousness of the conduct; (2) the circumstances surrounding the conduct, and the extent of knowledgeable participation; (3) how recent and frequent the behavior was; (4) the individual's age and maturity at the time of the conduct; (5) the voluntariness of participation; (6) the presence or absence of rehabilitation and other pertinent behavioral changes; (7) the motivation for the conduct; (8) the potential for pressure, coercion, exploitation, or duress; and (9) the likelihood of continuation or recurrence (See Directive, Section E2.2.1. of Enclosure 2). Because each security case presents its own unique facts and circumstances, it should not be assumed that the factors exhaust the realm of human experience or that the factors apply equally in every case. Moreover, although adverse information concerning a single condition may not be sufficient for an unfavorable determination, the individual may be disqualified if available information reflects a recent or recurring pattern of questionable judgment, irresponsibility, or other behavior specified in the Guidelines.

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.

Initially, the Government must establish, by substantial evidence, conditions in the personal or professional history of the applicant that disqualify, or may disqualify, the applicant from being eligible for access to classified information. The Directive presumes a nexus or rational connection between proven conduct under any of the disqualifying conditions listed in the guidelines and an applicant's security suitability. *See* ISCR Case No. 95-0611 at 2 (App. Bd. ay 2, 1996). All that is required is proof of facts and circumstances that indicate an applicant is at risk for mishandling classified information, or that an applicant does not demonstrate the high degree of judgment, reliability, or trustworthiness required of persons handling classified information. ISCR Case No. 00-0277, 2001 DOHA LEXIS 335 at **6-8 (App. Bd. 2001). Once the Government has established a *prima facie* case by substantial evidence, the burden shifts to the applicant to rebut, explain, extenuate, or mitigate the facts. *See* Directive ¶ E3.1.15. An applicant "has the ultimate burden of demonstrating that is clearly consistent with the national interest to grant or continue his security clearance. ISCR Case No. 01-20700 at 3 (App. Bd. 2002). "Any doubt as to whether access to classified information is clearly consistent with national security will be resolved in favor of the national security." Directive ¶ E2.2.2. "[S]ecurity clearance determinations should err, if they must, on the side of denials." *Egan*, 484 U.S. at 531. *See* Exec. Or. 12968 § 3.1(b).

Based upon a consideration of the evidence as a whole, I find the following adjudicative guidelines most pertinent to an evaluation of the facts of this case:

Guideline M: Misuse of Information Technology Systems: *The Concern: 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 communications, transmission, processing, manipulation, and storage of classified or sensitive information.* E2.A13.1.1

Guideline E: Personal Conduct: *The Concern: 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

Guideline D: Sexual Behavior: *The Concern: Sexual behavior is a security concern if it involves a criminal offense, indicates a personality or emotional disorder, may subject the individual to coercion, exploitation, or duress or reflects lack of judgment or discretion. Sexual orientation or preference may not be used as a basis for or a disqualifying factor in determining a person's eligibility for a security clearance*. E2.A4.1.1

CONCLUSIONS

The Government established by substantial evidence and Applicant's admissions each of the allegations in the SOR, including Paragraph 1.b. as amended. All the SOR allegations arise out of the unauthorized viewing of pornography on the government computers in 2003.

Regarding the Misuse of Information Technology Systems security concern contained in Guideline M, the Disqualifying Condition (DC) 3 (Use of hardware, software or media from any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations. E2.A13.1.2.3) Applicant used his government computer systems to view pornography during working hours. That use is prohibited by the DoD Directive cited.

Based on the facts that Applicant's misuse of Government computer systems to view pornography occurred regularly

over a six month period in June to December 2003, and it is now early 2006, Mitigating Condition (MC) 1 (The misuse was not recent or significant. E2.A13.1.3.1) applies. Applicant has now worked two years without a repeat of his past conduct. His former and current employers regard his work as exceptional. There is no specific test for recent actions in the guideline, and what is recent depends on the facts of the situation. Two years of solid performance that draws praise from both employers persuades me Applicant's behavior is in the past as regards using Government computer systems for the improper purpose. Therefore, I conclude this guideline for Applicant.

Regarding the Personal Conduct security concern, the applicable DC are DC 1 (Reliable, unfavorable information provided by associates, employers, coworkers, neighbors, and other acquaintances. E2.A5.1.2.1), DC 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. E2.A5.1.2.4), and DC 5 (A pattern of dishonesty or rule violations, including violation of any written or recorded agreement made between the individual and the agency. E2.A5.1.2.5). Applicant admitted he viewed pornography for a six-month period on government computers. That conduct violated the rule prohibiting such activity. His employer discovered it and provided such unfavorable information to the Government, leading to Applicant's job resignation. Applicant's repeated viewing of pornography at work makes him vulnerable to coercion, exploitation, or duress, particularly if he does it again at his new worksite.

Applicant now claims he will not view pornography during his work hours on government equipment. With that declaration, he is agreeing to do what he is required to do by rule, and he has supported that declaration by two years of exceptional performance for his new employer. These are positive steps Applicant has taken to reduce his vulnerability. MC 5 (The individual has taken positive steps to significantly reduce or eliminate vulnerability to coercion, exploitation, or duress. E2.A5.1.3.5) would apply. Lest anyone think no other MC could apply, my reading of the other MC under this Guideline E shows they apply more to the situation of falsification of government security forms that are not the allegation here. The personal conduct security concern is concluded for Applicant based on his project manager's strong statement on his behalf, Applicant's competent efforts at his new employment, and the fact the Government and his employer know of the previous incident.

Lastly, the Sexual Behavior guideline DC applicable are DC 3 (Sexual behavior that causes an individual to be vulnerable to coercion, exploitation, or duress. E2.A4.1.2.3) and DC 4 (Sexual behavior of a public nature and/or that which reflects lack of discretion or judgment. E2.A4.1.2.4). Using a government computer system to view pornography on a regular basis over a six-month time makes Applicant vulnerable and certainly shows a serious lack of discretion or judgment.

Under the facts presented, MC 2 (The behavior was not recent and there is no evidence of subsequent conduct of a similar nature. E2.A4.1.3.2), MC 3 (There is no other evidence of questionable judgment, irresponsibility, or emotional instability. E2.A4.1.3.3), and MC 4 (The behavior no longer serves as a basis for coercion, exploitation, or duress. E2.A4.1.3.4) apply. This incident is now more than two years old. The Government knows he looked at pornography while at work. Applicant says he won't do it again, and his current employer does not report any adverse situations or client complaints since Applicant came to work for that company in January 2004. There are no other incidents showing questionable judgment, irresponsibility or emotional instability since the incident, nor even prior to the incident at issue. There is nothing illegal about Applicant viewing pornography if he did it at home. The basis for potential coercion from his pornography viewing does not now exist within this context. Considering all of the evidence and applying the

"whole person concept" of the Directive, I conclude this security concern for Applicant.

FORMAL FINDINGS

The following are my conclusions as to each allegation in the SOR:

Paragraph 1. Guideline M: FOR APPLICANT

Subparagraph 1.a: For Applicant

Subparagraph 1.b: For Applicant

Paragraph 2. Guideline E: FOR APPLICANT

Subparagraph 2.a: For Applicant

Paragraph 3. Guideline D: FOR APPLICANT

Subparagraph 3.a: For Applicant

DECISION

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

Philip S. Howe

Administrative Judge

1. Pursuant to Exec. Or. 10865, *Safeguarding Classified Information within Industry* (Feb. 20, 1960), as amended and modified, and Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (Jan. 2, 1992), as amended and modified (Directive).