

DATE: January 29, 2004

In re:

SSN: -----

Applicant for Security Clearance

ISCR Case No. 02-12199

DECISION OF ADMINISTRATIVE JUDGE

JAMES A. YOUNG

APPEARANCES

FOR GOVERNMENT

Francisco Mendez, Esq., Department Counsel

FOR APPLICANT

Mark F. Riley, Esq.

SYNOPSIS

Based on purported admissions Applicant made to a polygrapher who interviewed him, the Defense Office of Hearings and Appeals issued a statement of reasons alleging Applicant downloaded pornographic images of children to his home computer and then deliberately falsified material facts about this conduct in a statement to a Defense Security Service agent. The National Security Agency refused to name the polygrapher or allow him to testify. The Government failed to establish by substantial evidence Applicant downloaded child pornography to his computer. 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 17 July 2003, DOHA issued a Statement of Reasons (SOR)⁽¹⁾, detailing the basis for its decision-security concerns raised under Guideline D (Sexual Behavior) and Guideline E (Personal Conduct) of the Directive. Applicant answered the SOR in an undated writing and elected to have a hearing before an administrative judge. The case was assigned to me on 27 October 2003. On 18 December 2003, I convened a hearing to consider whether it is clearly consistent with the national interest to grant or continue a security clearance for Applicant. DOHA received the transcript (Tr.) of the proceeding on 2 January 2003.

Applicant had a top secret clearance and applied for access to sensitive compartmented information (SCI)⁽²⁾. He was required to take a polygraph concerning possible counter-intelligence activities and his lifestyle. Subsequently, Applicant was denied access to SCI for downloading approximately 1,000 photographs of nude female children on his home computer. Exs. 2d, 2e. DOHA then issued an SOR concerning Applicant's access to any classified information.

At the hearing, over the objection of Applicant, the Government moved the admission of a document, labeled "Report," from a National Security Agency (NSA) polygrapher who interviewed Applicant. Ex. 2c for Identification. The report is unsigned and the name of the polygrapher does not appear on the document. The Chief, Security Information, Office of Personnel Security, National Security Agency, citing 50 U.S.C.A. §§ 402 note and 403-3(c)(6),⁽³⁾ asserted his Agency

"possesses an absolute statutory privilege against disclosing the identities of NSA employees or the security methods that the Agency employs to protect its sensitive intelligence sources and methods," and refused the Government's request to identify the polygrapher and allow him to testify.⁽⁴⁾

Applicants "shall be afforded an opportunity to cross-examine persons who have made oral or written statements adverse to the applicant relating to a controverted issue" unless "(1) the head of the Department supplying the statement certifies that the person who furnished the information is a confidential informant who has been engaged in obtaining intelligence information for the Government and that disclosure of his identity would be substantially harmful to the national interest; or (2) the head of the Department concerned or his designee has preliminarily determined that the statement appears to be reliable and material; failure to receive and consider the statement would, in view of the level of access sought, be substantially harmful to the national security ; and the person who furnished the information cannot appear to testify (A) due to death, severe illness, or similar cause, in which case the identity of the person and the information shall be made available to the applicant, or (B) due to some other cause determined by the head of the Department to be good and sufficient. Exec. Or. 10865 § 4. It appears the President has delegated the authority under to make a determination under § 4(2) to the General Counsel of the Department of Defense. Directive ¶ E3.1.22.2. The Government failed to establish either of the exceptions, and therefore, I denied admission of the document. *See* ISCR Case No. 95-0817, 1997 WL 377207 at *5 (App. Bd. Feb. 21, 1997).

FINDINGS OF FACT

Applicant, a 37-year-old network engineer, is married and has two children. Tr. 51-54. He has had a top secret clearance since 1995. Tr. 53.

As an employee of a defense contractor for the National Security Agency, Applicant applied for access to sensitive compartmented information (SCI). As part of the investigation for SCI access, Applicant was required to take a polygraph examination. During the suitability (also known as lifestyle) portion of the exam, the polygrapher noted an anomaly in the polygraph response to Applicant's denial of criminal conduct. Tr. 132. When Applicant was unsure what the problem could be, the polygrapher listed a number of different criminal offenses, one of which was child pornography. At the hearing, Applicant admitted telling the polygrapher that he "may have downloaded some child pornography" from the internet. Tr. 133. Applicant told the polygrapher that, between 1995 and 2000, he had downloaded pictures of naked women from the internet and some of these pictures were of naked children. The polygrapher asked whether it involved more or less than 1,000 pictures. Applicant replied, "Approximately 1,000." Tr. 134.

On 20 February 2002, Applicant completed a signed, sworn statement to a Defense Security Service (DSS) agent in which he clarified his activities in downloading nude photographs on his personal computer. Ex.4. Applicant claimed he downloaded well over 1,000 pictures of which approximately 20 happened to be of naked children. He asserted he was not interested in the images of children and immediately deleted them from his computer.

Applicant consulted a licensed psychologist prior to the hearing. The consultation consisted of six hours of clinical interview plus various psychological testing. The psychologist concluded Applicant did not have a personality disorder, but his "profile indicates that he is highly vulnerable to manipulation by authority due to a strong, even inordinate desire to please others and meet their expectations." Ex. F at 4.

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 restricted eligibility for access to classified information to United States citizens "whose personal and professional history affirmatively indicates loyalty to the United States, strength of character, trustworthiness, honesty, reliability, discretion, and sound judgment, as well as freedom from conflicting allegiances and potential for coercion, and willingness and ability to abide by regulations governing the use, handling, and protection of classified information." Exec. Or. 12968, *Access to Classified Information* § 3.1(b) (Aug. 4,

1995). Eligibility for a security clearance is predicated upon the applicant meeting the security guidelines contained in the Directive.

Enclosure 2 of the Directive sets forth personal 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.

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. *See Egan*, 484 U.S. at 531. 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. May 2, 1996).

Once the Government establishes a disqualifying condition by substantial evidence, the burden shifts to the applicant to rebut, explain, extenuate, or mitigate the facts. ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002); *see* Directive ¶ E3.1.15. 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.

CONCLUSIONS

Guideline D-Sexual Behavior

In the SOR, DOHA alleged Applicant downloaded up to 1000 pornographic images of children to his home computer. ¶ 1.a. An applicant's 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 a lack of judgment or discretion. Directive ¶ E2.A4.1.1.

On direct examination, Applicant asserted he told the polygrapher that he inadvertently downloaded "child pornography" through an automatic electronic newsreader while he was actually looking for pictures of naked women. He claimed that of the 1,000 to 2,000 pictures that were downloaded, only about 20 were of naked children and he immediately deleted them. He asserted he was not looking for pictures of children and none of the pictures, whether of adult women or children, were of sexually explicit acts. His testimony indicates the pictures may not even meet the legal definition of pornography. On cross-examination, through skillful questioning, the Department Counsel got Applicant to admit he told the polygrapher that, between 1995 and 2000, he had downloaded child pornography and there were approximately 1,000 pictures. Tr. 134. After carefully considering the context of the questions and answers, I conclude Applicant was referring to 1,000 pictures he claimed to have downloaded, not 1,000 pictures of child pornography.

The Government failed to establish by substantial evidence that Applicant downloaded child pornography to his home computer. Although Applicant admits using the term "child pornography," he reasonably claims he thought the term referred to any pictures of naked children. Even if the pictures contained child pornography, there is no evidence he deliberately downloaded the pictures of children. The Government failed to establish by substantial evidence any of the disqualifying conditions listed under Guideline D.

Guideline E-Personal Conduct

In the SOR, DOHA alleged Applicant deliberately falsified material facts in a sworn statement he submitted to a DSS agent when he claimed he had not intentionally searched for child pornography to download on his home computer (¶ 2.a.) and he downloaded up to 1,000 pornographic images of children to his home computer (¶ 2.b.). Conduct involving questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations could indicate the applicant may not properly safeguard classified information. Directive ¶ E2.A5.1.1.

Without evidence from the polygrapher about the contents of the interview, the Government was unable to establish by substantial evidence Applicant deliberately falsified his statement to the DSS agent or that he downloaded up to 1,000 pornographic images of children to his home computer. Thus, I must find for Applicant.

FORMAL FINDINGS

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

Paragraph 1. Guideline D: FOR APPLICANT

Subparagraph 1.a.: For Applicant

Paragraph 2. Guideline E: FOR APPLICANT

Subparagraph 2.a.: For Applicant

Subparagraph 2.b.: For Applicant

DECISION

While I am concerned about granting a security clearance to an applicant whose "profile indicates that he is highly vulnerable to manipulation by authority due to a strong, even inordinate desire to please others and meet their expectations," I am unable to find any disqualifying condition that would prevent him from holding a clearance. Thus, 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.

James A. Young

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,.
2. Pursuant to Director of Central Intelligence Directive 6/4, *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI)* (Oct. 13, 1999).
3. Apparently, the Chief, Security Information, was not aware that, two years before he signed the letter, § 403-3(c)(6) was redesignated § 403-3(c)(7). Pub. L. 107-56 § 901 (2001).
4. Actually, neither of the cited statutes provides such a statutory privilege for the NSA. There is a statutory privilege against disclosing identities of employees, but it appears to be limited to the Central Intelligence Agency, not the NSA. 50 U.S.C. § 403g. The Director of Central Intelligence does have, within the intelligence community, the authority to "protect intelligence sources and methods from unauthorized disclosure." 50 U.S.C. § 403-3(c)(7). However, an NSA polygrapher who conducts an interview concerning a security clearance is not an "intelligence source" and such an interview is not an intelligence "method" within the meaning of the statute. The notion that the NSA can defeat a Department of Defense inquiry into the security worthiness of an applicant who is performing contract labor for the NSA is dubious at best.