KEYWORD: Sexual Behavior; Personal Conduct

DIGEST: Based on purported admissions Applicant made to a polygrapher who interviewed him, the Defense Office of Hearings and Appeals declined to grant Applicant a clearance on grounds of sexual behavior and personal conduct. The statement of reasons alleged 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 deliberately downloaded child pornography to his computer. Clearance is granted.

CASENO: 02-12199.h2

DATE: 01/03/2005

DATE: January 3, 2005

In re:

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

Applicant for Security Clearance

ISCR Case No. 02-12199

REMAND 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 declined to grant Applicant a clearance on grounds of sexual behavior and personal conduct. The statement of reasons alleged 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 deliberately downloaded child pornography to his computer. Clearance is granted.

STATEMENT OF THE CASE

Applicant is an employee of a defense contractor holding contracts with the National Security Agency (NSA). Applicant held a top secret clearance and applied for access to sensitive compartmented information (SCI).[(1)] He was required to take a polygraph concerning possible counter-intelligence activities and his lifestyle. Thereafter, NSA denied Applicant access to SCI, finding he downloaded approximately 1,000 photographs of nude, female children on his home computer. Exs. 2d, 2e, 2f. NSA's action triggered a review of Applicant's eligibility for a security clearance. On 17 July 2003, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR),[(2)] detailing the basis for its decision that Applicant's security clearance should not be continued-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. On 29 January 2004, I issued a decision granting Applicant a clearance. The Government appealed. The Appeal Board remanded the case to me on 7 October 2004.

THE HEARING AND DECISION

At the hearing, Applicant objected to the admission of four government exhibits:

Ex. 2c for identification A document, labeled "Report," dated 16 November 2000, purportedly written by an NSA polygrapher who interviewed Applicant. The report is unsigned and the name of the polygrapher does not appear on the document.

Ex. 2d for identification Clearance decision statement from NSA's Office of Security, denying Applicant access to SCI, dated 11 July 2001.

Ex. 2g for identification NSA's First Appeal Review of the denial of Applicant's access to SCI, dated 3 October 2001.

Ex. 2i for identification NSA's Access Appeals Panel's decision, dated 24 January 2002, sustaining the denial of his access to SCI.

In Ex. 2c, the polygrapher claimed Applicant admitted purposely searching for child pornography 500 times on his home computer and downloading no more than 1,000 pornographic images of girls between 4 and 17 years of age in non-suggestive poses. Applicant asserted it was not an accurate summary of the interview. He claimed he downloaded pictures of nude adult women and that he immediately deleted the approximately 20 images of children that were included with the adult nudes. He objected to Ex. 2c for identification on two grounds. First, that the Government refused to produce or even identify the polygrapher so Applicant could exercise his right to cross-examination. Tr. 11 (citing Ex. Or. 10865 § 4); *see* Directive ¶ E3.1.22. Applicant also argued Ex. 2c for identification was a report of investigation that could not be received without an authenticating witness. *Id.*; *see* Directive ¶ E3.1.20. Department Counsel argued the polygrapher's statement was not a report of investigation (Tr. 16) and it was admissible as an exception to the hearsay rule under Fed. R. Evid. 803(6), 803(8), and 807 regardless of the availability of the witness.

I determined Ex. 2c for identification was a written statement adverse to Applicant relating to a controverted issue under Ex. Ord. 10865 § 4 and Directive ¶ E3.1.22, and was therefore not admissible without special certification from the head of the agency supplying the statement or from the General Counsel of the Department of Defense. I offered Department Counsel a continuance to seek such certification. After consultation with the Chief Department Counsel, he declined the offer. I sustained Applicant's objection to Ex. 2c.

Applicant's main objection to Exs. 2d, 2g, and 2i for identification was that they were decisions of NSA security official concerning Applicant's access to SCI that were based entirely on Ex. 2c for identification. Ex. 10. I admitted Exs. 2d, 2g, and 2i, for the limited purpose of establishing that NSA had denied Applicant access to SCI and the basis of that denial. I did not admit the documents as substantive evidence that Applicant committed the allegations described in the

SOR.

In a decision dated 29 January 2004, I granted Applicant a clearance because the Government failed to establish facts that would disqualify Applicant from a security clearance. Department Counsel appealed.

THE REMAND

In a decision dated 7 October 2004, the Appeal Board sustained my conclusion that Ex. 2c for identification was not admissible under Directive ¶ E3.1.22, but was a "report of investigation" and ordered me to consider its admissibility under Directive ¶ E3.1.20. ISCR Case No. 02-12199 at 6, 10 (App. Bd. Oct. 7, 2004). The Board also determined Exs. 2d, 2g, and 2i were not "reports of investigation" and ordered me to consider their admissibility under Directive ¶¶ E3.1.20 and E3.1.22.

THE CASE ON REMAND

Pursuant to the Board's direction, I gave the parties an opportunity to submit written briefs on the admissibility of the evidence. Both parties did so.

Ex. 2c for identification

In its decision, the Appeal Board concluded that Ex. 2c "is a report of an NSA investigation of Applicant" and, since Applicant objected to its admissibility, Department Counsel was required to satisfy the requirements of Directive ¶ E3.1.20 before it could be admitted into evidence. ISCR Case No. 02-12199 at 8 (App. Bd. Oct. 7, 2004). Directive ¶ E3.1.20 permits a report of investigation (ROI) to be admitted into evidence "with an 'authenticating witness' provided it is otherwise admissible under the Federal Rules of Evidence."

At the hearing, the Government did not produce an authenticating witness for Ex. 2c for identification. Thus, Ex. 2c for identification was not admissible. The Appeal Board authorized the reopening of the record so the parties could present pertinent evidence on this issue, if I determine the party has made a showing of "good cause." *Id.* at 10. Department Counsel attached an affidavit from the NSA records custodian to his remand brief, claiming the affidavit--certifying that the four exhibits in question were accurate copies of documents generated and kept in the regular course of business--constitutes good cause to reopen the record.[(3)]

The Appeal Board has not fully defined the term "good cause." "Good cause" is the burden placed on a litigant to show why a request should be granted or an action excused. *Black's Law Dictionary*, "Cause" (8th ed. 2004). There is nothing in the record custodian's affidavit or Department Counsel's brief that explains why I should reopen the record to consider the affidavit. The Appeal Board has suggested that in determining whether a party has shown "good cause," the judge should consider such factors as "the timing of the request, the nature of the request, and the extent to which the moving party had an earlier opportunity to proffer the arguments." ISCR Case No. 99-0018, 2000 WL 739496 (App. Bd. Apr. 11, 2000). Department Counsel had an earlier opportunity to present an "authenticating witness," but instead argued the polygrapher's statement was not an ROI and therefore not covered by Directive ¶ E3.1.20. Tr. 16. Department Counsel has not offered any justification for the Government's failure to offer the affidavit or an authenticating witness at the hearing. After considering all the circumstances, I conclude Department Counsel failed to establish good cause to reopen the record to admit the affidavit. Without authentication, the ROI is not admissible. Thus, Department Counsel failed to establish the admissibility of Ex. 2c for identification under Directive ¶ E3.1.20.

Exs. 2d, 2g, and 2i

At the hearing, I admitted Exs. 2d, 2g, and 2i for the limited purpose of establishing that NSA had denied Applicant access to SCI and the basis for its decision. Nevertheless, the Appeal Board ordered me to consider the admissibility of Exs. 2d, 2g, and 2i under Directive ¶¶ E3.1.20 and E3.1.22. The Appeal Board determined that Exs. 2d, 2g, and 2i are not reports of investigation. ISCR Case No. 02-12199 (App. Bd. Oct. 7, 2004).

Exs. 2d, 2g, and 2i are not written statements adverse to the applicant on a controverted issue. They are instead the decisions of various security officials at NSA on Applicant's request for access to SCI. Ex. 2d, the initial SCI clearance decision statement, does contain substantial excerpts from Ex. 2c for identification, the polygrapher's summary of his interview with Applicant, but that does not make Ex. 2d a "statement." Therefore, I conclude Directive ¶ E3.1.22 does not apply.

Exs. 2d, 2g, and 2i are clearly official records created in the regular course of business that have been furnished by an investigative agency pursuant to its responsibilities to assist the Department of Defense and the NSA to safeguard classified information. They are admissible, therefore, under Directive ¶ E3.1.20. But the question remains, for what purposes? Are these documents admissible to show Applicant downloaded child pornography or are they admissible

only for the limited purpose of showing what NSA decided regarding Applicant's request for access to SCI and the basis of that decision?

In DOHA proceedings, "[r]elevant and material evidence may be received subject to rebuttal, and technical rules of evidence may be relaxed, *except as otherwise provided herein*, to permit the development of a full and complete record." Directive ¶ E3.1.19 (emphasis added). Hearsay evidence is admissible and may constitute substantial evidence if it appears reliable. *See Hoska v. Dept. of the Army*, 677 F.2d 131, 138-39 (D.C. Cir. 1982); ISCR Case No. 01-12429, 2003 WL 21371603 (App. Bd. Jan. 15, 2003); Gary J. Edles & Jerome Nelson, *Federal Regulatory Process: Agency Practices and Procedures* 153 (2d ed. 1995). *Cf. Richardson v. Perales*, 402 U.S. 389, 402 (1971) (holding reports of doctors were admissible and constituted substantial evidence despite the hearsay nature of the reports and lack of cross examination, when the Social Security claimant did not exercise his right to subpoena the reporting physicians and thereby provide himself with the opportunity for cross-examination. The identify of the five reporting physicians was a significant factor in the Court's decision.).

The information in Exs. 2d, 2g, and 2i, concerning Applicant's downloading child pornography, is hearsay if offered to prove Applicant deliberately downloaded child pornography. Applicant demanded the polygrapher who provided that information testify at the hearing. Applicant did not have subpoena power to force attendance of the polygrapher. Citing a letter from the Chief, Security Information, Office of Personnel Security, National Security Agency (Ex. 8), Department Counsel refused to identify or make the polygrapher/declarant of Ex. 2c for identification available to testify because the witness was "not within [Department Counsel's] control." Ex. 9.

In the letter, the Chief, Security Information, asserted NSA "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." Ex. 8 (citing 50 U.S.C.A. §§ 402 note and 403-3(c)(6)).[(4)]

Neither of the cited statutes provides such a privilege for NSA. There is a statutory privilege against disclosing identities of employees, but it appears to be limited to the Central Intelligence Agency. 50 U.S.C. § 403g. The Director of Central Intelligence (DCI) 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. There is also no evidence the DCI exercised his authority to protect this polygrapher as an "intelligence source."[(5)]

I conclude the polygrapher's report, as excerpted and referenced in Exs. 2d, 2g, and 2i, has not been shown to be reliable hearsay. Applicant was unable to cross-examine the polygrapher because the Government did not make him available. By refusing to disclose the polygrapher's identity, the Government precluded Applicant from impeaching him. *See* Fed. R. Evid. 806 (a hearsay declarant may be attacked by any evidence which would be admissible for those purposes if declarant had testified as a witness). We know nothing about the polygrapher. We do not know if he has made allegations that proved false in the past. We do not even know if the polygrapher's report was made contemporaneously with the interview. Under the circumstances, there is no basis to conclude the polygrapher's report is reliable.

In addition, Directive ¶ E3.1.20 placed specific limitations on the admissibility of ROIs. To allow the Government to avoid these limitations by the simple expedient of summarizing the ROI in another letter or report would eviscerate the rule. Accordingly, Exs. 2d, 2g, and 2i are not admissible substantively under Directive ¶ E3.1.20.

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 an 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 before 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 1,000 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, 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.l.l.

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. 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, 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

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 Director of Central Intelligence Directive 6/4, *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI)* (Oct. 13, 1999).

2. 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.

3. As the Appeal Board stated, Ex. 2c for identification is not admissible absent an authenticating witness. Directive ¶ E3.1.20. I doubt an affidavit from a records custodian qualifies as a "witness." If the drafters had meant to apply the self-authentication rules of Fed. R. Evid. 901 and 902, they would have mentioned affidavits as a means of authenticating the ROI. On the other hand, what can a records custodian testify to that cannot be put into an affidavit? Regardless, as Department Counsel failed to show good cause, this issue is left for another day.

4. 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).

5. 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.