DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 12-02296
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Julie R. Mendez, Esquire, Department Counsel
For Applicant: *Pro se*

01/03/2014

Decision

METZ, John Grattan, Jr., Administrative Judge:

Based on the record in this case,[1] Applicant's clearance is denied.

On 19 June 2013, the Department of Defense (DoD) issued a Statement of Reasons (SOR) to Applicant detailing security concerns under Guidelines E, (Personal Conduct), D (Sexual Behavior), and M (Use of Information Technology Systems).[2] Applicant timely answered, requesting a hearing before the Defense Office of Hearings and Appeals (DOHA). DOHA assigned the case to me 6 August 2013, and I convened a hearing 28 August 2013. DOHA received the transcript (Tr.) 4 September 2013.

[1]Consisting of the transcript (Tr.), Government exhibits (GE) 1-3, and Applicant exhibit (AE) A.

[2]DoD acted under Executive Order 10865, *Safeguarding Classified Information within Industry* (February 20, 1990), as amended; DoD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the adjudicative guidelines (AG) effective within the DoD on 1 September 2006.

Findings of Fact

Applicant admitted the SOR allegations. He is a 37-year-old senior consultant employed by a defense contractor since August 2011. He seeks to regain the clearance he held until he was terminated for cause from his previous employment in April 2011. He first obtained a clearance in approximately May 2001.

In April 2011, Applicant was fired from a job he had held since September 2003 for spending excessive amounts of time on the internet for non-business purposes (including pornographic websites), then charging the non-business time to Government contracts (GE 2, 3). Applicant had been counseled on numerous occasions concerning the viewing of inappropriate material using company computer systems.

Applicant was unemployed for about four months, when he obtained his current position. In his September 2011 clearance application (GE 1), although he disclosed his employment with the prior company, he failed to disclose that he had been fired from that employment. He affirmatively misrepresented the circumstances of this departure by stating that he had left the company because of "loss of contract/work." In December 2011, he gave conflicting explanations to the Government investigator (AE B). He claimed that he did not list his firing because of an oversight, but he also claimed that he failed to list his termination because it was the lack of work at the company that gave him the free time for personal use of the company computer.

Applicant's past and current work references consider him honest and trustworthy, and recommend him for his clearance (AE A). However, only one of them appears to be aware of the circumstances of his firing from his prior employment.

Policies

The adjudicative guidelines (AG) list factors to evaluate a person's suitability for access to classified information. Administrative judges must assess disqualifying and mitigating conditions under each issue fairly raised by the facts and situation presented. Each decision must also show a fair, impartial, and commonsense consideration of the factors listed in AG ¶ 2(a). The applicability of a disqualifying or mitigating condition is not, by itself, conclusive. However, specific guidelines should be followed when a case can be measured against them, as they are policy guidance governing the grant or denial of a clearance. Considering the SOR allegations and the evidence as a whole, the relevant adjudicative guideline is Guideline E (Personal Conduct), Guideline D (Sexual Behavior), and Guideline M (Use of Information Technology Systems).

Security clearance decisions resolve whether it is clearly consistent with the national interest to grant or continue an applicant's security clearance. The Government must prove, by substantial evidence, controverted facts alleged in the SOR. If it does, the burden shifts to applicant to refute, extenuate, or mitigate the Government's case. Because no one has a right to a security clearance, the applicant bears a heavy burden of persuasion.

Persons with access to classified information enter into a fiduciary relationship with the Government based on trust and confidence. Therefore, the Government has a compelling interest in ensuring each applicant possesses the required judgement, reliability, and trustworthiness of those who must protect national interests as their own. The "clearly consistent with the national interest" standard compels deciding any reasonable doubt about an Applicant's suitability for access in favor of the Government.[3]

Analysis

The Government established a case for disqualification under Guideline E, and Applicant did not mitigate the security concerns. Applicant breached his fiduciary duty to his employer and to the Government, for which he was properly terminated from employment.[4] Further, he compounded this astoundingly poor judgment by deliberately failing to disclose this termination and actively misrepresenting his reason for leaving the company.[5]

None of the Guideline E mitigating conditions apply. The concealed and misrepresented information was relevant and material to a clearance decision. Applicant did not disclose this information until his subject interview. The Government has an interest in examining all relevant and material adverse information about an applicant before making a clearance decision. The Government relies on applicants to truthfully disclose that adverse information in a timely fashion, not when they perceive disclosure to be prudent or convenient. Further, an applicant's willingness to report adverse information about himself provides some indication of his willingness to report inadvertent security violations or other security concerns in the future, something the Government relies on to perform damage assessments and limit the compromise of classified information. Applicant's conduct suggests he is willing to put his personal needs ahead of legitimate Government interests. Accordingly, I resolve Guideline E against Applicant. Whole-person considerations require no different result.

---

[3] *See*, *Department of the Navy v. Egan*, 484 U.S. 518 (1988).

[4] ¶ 16.(c) credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any other single guideline, but which, when considered as a whole, supports a whole person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the person may not properly safeguard protected information; (d) credible adverse information that is not explicitly covered under any other guideline and may not be sufficient by itself for an adverse determination, but which, when combined with all available information supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the person may not properly safeguard protected information. . . ;

[5] ¶ 16(a) deliberate omission, concealment, or falsification of relevant and material facts from any personnel security questionnaire, personal history statement, or similar form used to conduct investigations, . . . [or] determine security clearance eligibility or trustworthiness. . .; (b) deliberately providing false or misleading information regarding relevant facts to an . . . investigator . . .;

The Government failed to establish a case for disqualification under Guideline D. The Government's evidence did not establish that Applicant's viewing of pornographic websites was criminal,[6] constituted a pattern of problematic sexual behavior,[7] caused him to be subject to coercion, exploitation, or duress,[8] or was public in nature.[9] Applicant's poor judgment consisted of using company time and resources for non-business purposes, and then charging that time to Government contracts. Applicant's viewing of pornographic websites is part of that non-business use, but the marginal increase in poor judgment, if any, does not support revocation of Applicant's clearance on this ground. Accordingly, I resolve Guideline D for Applicant.

Similarly, the Government failed to establish a case for disqualification under Guideline M. Again, Applicant's misconduct consisted of using company time and resources for non-business purposes, and then charging that time to Government contracts. The Government produced no evidence that company policy otherwise prohibited Applicant's use of company computers for non-business purposes, to include viewing legal sexual content, provided that the use occurred on his own time. Applicant's misconduct certainly violated company policies addressed most appropriately under Guideline E, but his misuse of company time and resources do not implicate information technology per se. That misconduct did not constitute illegal or unauthorized entry,[10] illegal or unauthorized modification,[11] use of a system to gain unauthorized access to other systems,[12] unauthorized transfer of classified information,[13] unauthorized use of a government or other information technology

[6]¶ 13(a) sexual behavior of a criminal nature, whether or not the individual has been prosecuted;

[7]¶ 13(b) a pattern of compulsive, self-destructive, or high-risk sexual behavior that the person is unable to stop or that may be symptomatic of a personality disorder;

[8]¶ 13(c) sexual behavior that causes an individual to be vulnerable to coercion, exploitation, or duress;

[9]¶ 13(d) sexual behavior of a public nature and/or that reflects lack of discretion or judgment.

[10]¶ 40(a) illegal or unauthorized entry into any information technology system or component thereof;

[11]¶ 40(b) illegal or unauthorized modification, destruction, manipulation, or denial of access to information, software, firmware, or hardware in an information technology system;

[12]¶ 40(c) use of any information technology system to gain unauthorized access to another system or to a compartmented area within the same system;

[13]¶ 40(d) downloading, storing, or transmitting classified information on or to any unauthorized software, hardware, or information technology system;

system,[14] unauthorized tampering with system components,[15] lax security habits,[16] or misuse resulting in damage to the national security.[17] Accordingly, I resolve Guideline M for Applicant.

Formal Findings

Paragraph 1. Guideline E:	AGAINST APPLICANT
Subparagraphs a-b:	Against Applicant
Paragraph 2. Guideline D:	FOR APPLICANT
Subparagraph a:	For Applicant
Paragraph 3. Guideline M:	FOR APPLICANT
Subparagraph a:	For Applicant

Conclusion

Under 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. Clearance denied.

JOHN GRATTAN METZ, JR
Administrative Judge

[14]¶ 40(e).

[15]¶ 40(f) introduction, removal, or duplication of hardware, firmware, software, or media to or from any information technology system without authorization, when prohibited by rules, procedures, guideline, or regulations;

[16]¶ 40(g) negligence or lax security habits in handling information technology that persist despite counseling by management;

[17]¶ 40(h) any misuse of information technology, whether deliberate or negligent, that results to damage to the national security.