DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 08-06951
SSN:	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Tovah Minster, Esquire, Department Counsel
For Applicant: Joël Van Over, Esquire

September 24, 2010

Decision

METZ, John Grattan, Jr., Administrative Judge:

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

On 23 June 2009 the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) to Applicant detailing security concerns under Guideline E, Personal Conduct.[2] Applicant timely answered, and requested a hearing. DOHA assigned the case to me 31 August 2009, and I convened a hearing 29 September 2009. DOHA received the transcript 7 October 2009.

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

[2]DOHA acted under Executive Order 10865, *Safeguarding Classified Information within Industry* (February 20, 1990), as amended; Department of Defense (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, except for SOR 1.f. He is a 42-year-old practice technical lead employed by a defense contractor since October 1996. He seeks reinstatement of the security clearance he has held since October 1997.

Applicant graduated from college in May 1985. He married in October 1989, and has two children, ages 17 and 14.

After Applicant went to work for his employer in October 1996, he applied for his first clearance, which he obtained in October 1997. In January 2002, he was subject to periodic reinvestigation, and his clearance was renewed in May 2003 (AE B).[3] He handled classified information, as necessary, without incident.

After Applicant's clearance was granted in October 1997, most of his work was for one government agency. From 1997 to 2005, Applicant took government computer equipment from his workplace without authorization. He was aware of the requirement to have a property pass to take government equipment out of the building because he had obtained property passes in the past to take government equipment to trade shows. Applicant initially gave no reason for his failure to get authorization (Tr. 43-44), but later on he realized no one ever checked to see if he had a property pass (Tr. 49).

Applicant mostly took government equipment home to familiarize himself with it to better perform his work. He usually returned the equipment within a few weeks, but in some instances kept it much longer when it became apparent that the equipment was not going to be used in his work. Applicant generally did not use the equipment for personal reasons, but did use a digital camera to take family pictures. Applicant estimates he took home over $1,300 worth of government property.

Applicant also took home items the government agency had thrown in the trash: compact discs and video discs, some with non-sensitive test data on them, some blank. He took home an unopened copy of reinstallation software that had also been thrown in the trash.[4] He had the same operating system on his home computer, and while he had a valid license for his software, his reinstallation disc was defective. He used the

[3]The government clearance database contained in AE B records only the dates of background investigations, subsequent adjudications of those investigations, the level of clearance granted, and terminations of clearances, either administratively or for cause. The database does not record access to classified information. Each agency makes its own assessment of whether an individual should be given access to classified information, and at what level. Agencies are also the sole arbiters of which individuals should be given special or additional access to information designated for greater protection than that provided by the basic classifications.

[4]Government computer systems generally are delivered with the necessary software, particularly the operating systems, pre-loaded. The government purchases a license to use each copy of the software, which frequently means that multiple copies of the reinstallation discs are delivered with the computer systems. Government technical support is such that the discs are seldom needed.

government-purchased software to reload the program on his computer, using his valid license to register the program with the software company.

This misuse of government property came to light when Applicant underwent a polygraph examination in June 2005. While Applicant's work with the original government agency was wrapping up in 2004, his company nominated him to work on a contract with a different government agency, one which required its contractors to pass a lifestyle polygraph before receiving final approval for the additional access needed to work on the contract. This agency did not schedule Applicant's polygraph until June 2005. The initial polygraph raised some issues that the agency wanted to address, and he was polygraphed again a week later.

During the polygraphs, Applicant disclosed the misuse of government property described above as well as a lengthy history of mild "road rage" incidents. From 1990 to 2005, Applicant "keyed" the automobiles of drivers who Applicant considered to have driven dangerously. He did this only when the offending driver parked in the same parking lot as Applicant; he never followed the drivers to a different location from where he was heading. Applicant has given varying estimates of the number of times he "keyed" automobiles. The polygrapher recorded 6-15 times—the number alleged in the SOR—most recently about a month before his polygraph. Applicant unequivocally admitted this allegation. However, during a subject interview in June 2007, Applicant stated fewer than 10 times as a more accurate number (GE 3). At hearing, he testified that 6-10 times was a more accurate number (Tr. 67).

In November 2005, the government agency disapproved Applicant for additional access and revoked his existing access (GE 2). The agency raised issues under criminal conduct and personal conduct. The agency specified the misconduct cited above, as well as the agency's assessment that Applicant had not been candid during security processing because Applicant reported his misconduct in a piecemeal manner. In January 2006, Applicant requested review of the decision, but the decision was affirmed in December 2006. Applicant did not file a second-level appeal. He was taken off the agency contract and assigned to other contracts. It does not appear that Applicant's company security office was aware of, or involved in, this reassignment. Applicant did not provide his facility security officer (FSO) with copies of the correspondence between him and the government agency concerning the denial and revocation of his access (Tr. 108).

The government's clearance database (AE B) administratively terminated his clearance in March 2007 for loss of jurisdiction, i.e., no longer employed in a job requiring a clearance. Although the entry shows that it was an incident report adjudication, there is no evidence to conclusively connect the administrative termination of Applicant's clearance with the agency adjudications of his access to agency information.

In March 2007, Applicant completed another clearance application for his periodic reinvestigation (GE 1). Applicant answered "no" to a question (26b) requiring

him to disclose if he had ever had a clearance or access authorization denied, suspended, or revoked. Applicant denies intending to falsify his clearance application, variously claiming that the omission was an "oversight" (Tr. 86) or that he was only focused on the "clearance" aspect of the question (Tr. 93). I find neither claim credible. The March 2007 clearance application was at least his third such application in 11 years, so he was well familiar with the forms and the process. The language of the question is straightforward, and Applicant answered it three months after receiving the last letter from the agency affirming the denial and revocation of his access. Finally, Applicant never gave his FSO copies of those letters, suggesting that he did not want the company to know of the agency action.

The company did not become aware of the termination of Applicant's clearance until November 2008, when his FSO noticed the database entry while processing a routine visit request. The FSO took the appropriate steps to notify the appropriate clients that Applicant no longer had a clearance, and therefore no longer had access, but it appears that at least one incorrect visit request was processed before November 2008.

Applicant's work reference considers him honest and trustworthy, and recommends him for his clearance (Tr. 139-146). He considers the misconduct noted in the SOR inconsistent with what he knows of Applicant. Applicant advised him of the misconduct the week before the hearing (Tr. 146).

Policies

The adjudicative guidelines (AG) list factors to be used to evaluate an applicant's suitability for access to classified information. Administrative judges must assess both disqualifying and mitigating conditions under each issue fairly raised by the facts and situation presented. Each decision must also reflect a fair, impartial, and commonsense consideration of the factors listed in AG ¶ 2(a). The presence or absence of a disqualifying or mitigating condition is not, by itself, conclusive. However, specific guidelines should be followed where a case can be measured against them, as they represent 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).

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. As no one has a right to a 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 requisite judgement, reliability, and trustworthiness of those who must protect national interests as their own.

The "clearly consistent with the national interest" standard compels resolution of any reasonable doubt about an applicant's suitability for access in favor of the Government.[5]

Analysis

The Government established a case for disqualification under Guideline E, and Applicant did not mitigate the security concerns. Applicant falsified his March 2007 clearance application by failing to disclose that another government agency denied and revoked his special access to that agency's information in December 2006. The agency's adverse access determination was based, in part, on Applicant providing disqualifying information in a piecemeal fashion.[6] In addition, Applicant took government property from his workplace to his home for personal use, without authorization, and without returning it in a timely manner. He also engaged in vigilante vandalism for about 15 years.[7] Thus, the burden of persuasion shifted to Applicant to refute or mitigate the government's information.

There are two separate, but intertwined, threads of disqualifying conduct. First, Applicant has shown his willingness to hide adverse information from the Government by falsifying his March 2007 clearance application. This misconduct cannot be considered an aberration because it occurs against the background of having not made complete disclosure of information during his polygraph examinations, his failing to disclose the agency access determination to his company clearance office, and his waiting until the week before the hearing to disclose the SOR allegations to his character witness.

The other disqualifying thread is Applicant's willingness to decide for himself what government requirements and societal norms he will follow—in effect substituting his

---

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

[6] ¶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 . . .;

[7] ¶ 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. . . ; (e) personal conduct, or concealment of information about one's conduct, that creates a vulnerability to exploitation, manipulation, or duress, such as (1) engaging in activities which, if known, may affect the person's personal, professional, or community standing . . .;

judgment. He misappropriated government equipment.[8] He determined for himself which "dangerous" drivers were to be punished by his vigilante vandalism—itself minor criminal conduct. I have considered that both forms of misconduct ceased in 2005 when it surfaced during his polygraph examinations, that he has handled classified information without incident since his first clearance in 1997, and that his work reference considers him trustworthy and reliable. However, I find this favorable information inadequate to overcome the adverse implications of his misconduct under Guideline E or to warrant a favorable result under a whole-person analysis. I resolve Guideline E against Applicant.

Formal Findings

Paragraph 1. Guideline E:	AGAINST APPLICANT
Subparagraphs a-f:	Against Applicant

Conclusion

In light of all 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

[8]However, I consider the electronic media and computer program taken from the trash can as having been abandoned by the government agency, and thus not indicative of any misconduct by Applicant. Nevertheless, the other government property taken by Applicant is enough to warrant denial of his clearance.