KEYWORD: Information Technology; Personal Conduct

DIGEST: Applicant's misuse of his government computer on multiple occasions from 1998 to 2000, and his December 2001 false statement about the circumstances of that misuse, demonstrated that he lacks the judgment, reliability, and trustworthiness required of those with access to classified information. Clearance denied.

CASENO: 02-17345.h1

DATE: 04/10/2006

DATE: April 10, 2006

In Re:

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

Applicant for Security Clearance

ISCR Case No. 02-17345

DECISION OF ADMINISTRATIVE JUDGE

JOHN GRATTAN METZ, JR

APPEARANCES

FOR GOVERNMENT

Eric H. Borgstrom, Esquire, Department Counsel

FOR APPLICANT

Pro Se

SYNOPSIS

Applicant's misuse of his government computer on multiple occasions from 1998 to 2000, and his December 2001 false statement about the circumstances of that misuse, demonstrated that he lacks the judgment, reliability, and trustworthiness required of those with access to classified information. Clearance denied.

STATEMENT OF THE CASE

Applicant challenges the 4 December 2003 Defense Office of Hearings and Appeals (DOHA) Statement of Reasons (SOR) recommending denial or revocation of his clearance because of misuse of information technology systems and personal conduct.[(1)] He answered the SOR 13 January 2004, and requested a decision without hearing. He did not respond to DOHA's 31 October 2005 File of Relevant Material (FORM). The record closed 29 December 2005, when his response was due. DOHA assigned the case to me 23 January 2006.

PROCEDURAL ISSUES

In the FORM, Department Counsel moved to amend the SOR to add subparagraphs 2.c., falsification of a December

2001 sworn statement, and 2.d., denial of SCI access by a government agency in October 2003. The record evidence supports the amendment and, accordingly, I grant the motion. Applicant having not responded to the FORM, I formally enter his denial of the allegation, consistent with his answer to the original SOR.

FINDINGS OF FACT

Applicant denied the allegations of the SOR.

Applicant--a 52-year-old director of a defense contractor since July 2001--seeks an industrial security clearance. He is a retired U.S. Army colonel (paygrade O-6), who had a clearance during the 26 years he spent on active duty.

Between 1998 and 2000, Applicant deliberately accessed pornographic websites multiple times on his government-issued, unclassified laptop computer, in violation of government regulations. Applicant claims that he was unaware of the prohibition against accessing pornographic websites when he first accessed the sites, a claim that is not credible given his length of service in the Army and his assignment as a senior officer in the senior logistics policy organization in the Army when the misuse occurred.

Unbeknownst to Applicant, the government monitored his computer for just such misuse of government computers, and he was confronted by his supervisor after he had accessed pornographic websites 10-20 times. His supervisor told him to stop accessing pornographic websites on his government computer. Nevertheless, Applicant continued to access pornographic websites and he was counseled again by his supervisor and told to stop his misuse of his computer. Applicant still used his government computer to access pornographic websites. Computer monitoring systems registered hundreds of "hits" on pornographic websites. On each occasion that Applicant was counseled, he signed an acknowledgment that he was not to access pornographic websites in the future.

Applicant denies that he visited these websites to satisfy any prurient interests of his own, but because he knew that his teenage son was accessing pornographic websites on the family's home computer and Applicant was trying to devise a strategy to prevent his son's access without his son knowing that the father knew. Several factors undercut this stated intention. First, Applicant eventually ended his son's access to the family computer, yet he continued to access pornographic websites after this date. Second, the Army reported finding a hole punched into the wall below Applicant's computer between Applicant's office and an adjacent office with a telephone (modem) line running into the next office. This suggests that Applicant sought to conceal his continued accessing of pornographic websites. Finally, the Army reported that Applicant scrubbed the hard drive of his government-issued laptop before turning it in to the Army when he retired in April 2001, preventing the Army from learning if Applicant had downloaded pornographic images onto the computer. In addition, Applicant's computer was found to have unauthorized internet software loaded onto it. Applicant

has, at various times, claimed that the software was loaded by IT personnel at his work or perhaps by his son, who had access to the computer when Applicant took it home.

In 2001, Applicant was sponsored for SCI (Special Compartmented Information) access in his current position, a process that required--among other things--satisfactory completion of a polygraph examination. In December 2001, Applicant gave a sworn statement in which he falsely claimed that he had not accessed pornographic websites after his first counseling, except for inadvertently visiting www.whitehouse.com when he was looking for www.whitehouse.gov, which caused the second counseling session. In a March 2002 sworn statement to a DSS polygrapher, he disclosed that he had continued to access pornographic websites after both counseling sessions. In October 2003, the federal agency with whom Applicant had sought SCI access denied his request.

POLICIES AND BURDEN OF PROOF

The Directive, Enclosure 2 lists adjudicative guidelines to be considered in evaluating an Applicant's suitability for access to classified information. Administrative Judges must assess both disqualifying and mitigating conditions under each adjudicative issue fairly raised by the facts and circumstances presented. Each decision must also reflect a fair and impartial common sense consideration of the factors listed in Section 6.3. of the Directive. The presence or absence of a disqualifying or mitigating condition is not determinative for or against Applicant. However, specific adjudicative guidelines should be followed whenever a case can be measured against them, as they represent policy guidance governing the grant or denial of access to classified information. Considering the SOR allegations and the evidence as a whole, the relevant, applicable, adjudicative guidelines are Guideline M (Misuse ITS) and 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 something less than a preponderance of the evidence, controverted facts alleged in the SOR. If it does so, it establishes a *prima facie* case against access to classified information. Applicant must then 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 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.[(2)]

CONCLUSIONS

The government has established its case under Guideline M, and Applicant has not mitigated the conduct. Applicant accessed pornographic websites on his government-issued laptop multiple times between 1998 and 2000, in violation of government policies.(3) He continued to do so after being counseled on two separate occasions to stop accessing pornographic sites. He also installed internet software on his laptop without permission.(4)

Applicant meets none of the mitigating conditions for misuse of ITS. His misuse was both recent and significant.(5) His misuse was deliberate, and continued after specific direction to stop.(6) Applicant failed to corroborate his claim that government employees had installed the internet software on his computer.(7) He also provided no evidence that his son loaded the software--which in any event would be attributed to Applicant. His misuse continued for over two years.(8) He took no action to correct his misuse.(9) Accordingly, I resolve Guideline M against Applicant.

The government established a Guideline E case, and Applicant has not mitigated the security concerns. In addition to the misuse of his computer over several years,(10) Applicant deliberately falsified a December 2001 sworn statement by claiming that he had stopped accessing pornographic websites after his first counseling, when he had continued to access pornographic websites after both warnings.(11) He did not reveal the full extent of his computer misuse until his polygraph interview. Further, none of the Guideline E mitigating conditions apply. The concealed information was relevant to a clearance decision.(12) The falsifications were not isolated, they were recent, and the Applicant did not provide the correct information voluntarily.(13) He did not correct the falsification before being confronted with it.(14) There is no evidence suggesting Applicant received bad advice about what he was required to disclose.(15) I conclude Guideline E against Applicant.

FORMAL FINDINGS

Paragraph 1. Guideline M: AGAINST APPLICANT

Subparagraph a: Against Applicant

Subparagraph b: Against Applicant

Paragraph 2. Guideline E: AGAINST THE APPLICANT

Subparagraph a: Against Applicant

Subparagraph b: Against Applicant

Subparagraph c: Against Applicant

Subparagraph d: Against Applicant

DECISION

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

1. Required by Executive Order 10865 and Department of Defense Directive 5220.6, as amended (Directive).

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

3. E2.A13.1.2.1. Illegal or unauthorized entry into any information technology system; E2.A13.1.2.3.Removal (or use) of hardware, software or media from any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations;

4. E2.A13.1.2.4. Introduction of hardware, software or media into any information technology system with authorization, when specifically prohibited by rules, procedures, guidelines or regulations;

5. E2.A13.1.3.1. The misuse was not recent or significant ;

6. E2.A13.1.3.2. The misuse was unintentional or inadvertent;

7. E2.A13.1.3.3. The introduction or removal of media was authorized;

8. E2.A13.1.3.4. The misuse was an isolated event;

9. E2.A13.1.3.5. The misuse was followed by a prompt, good faith effort to correct the situation.

10. E2.A5.1.2.1. Reliable, unfavorable information provided by associates, employers, coworkers, neighbors, and other acquaintances;

11. E2.A5.1.2.3. Deliberately providing false or misleading information concerning relevant and material matters to an investigator, security official, competent medical authority, or other official representative in connection with a personnel security or trustworthiness determination;

12. E2.A5.1.3.1. The information was unsubstantiated or not pertinent to a determination of judgment, trustworthiness, or reliability;

13. E2.A5.1.3.2. The falsification was an isolated incident, was not recent, and the individual has subsequently provided correct information voluntarily;

14. E2.A5.1.3.3. The individual made prompt, good-faith efforts to correct the falsification before being confronted with the facts;

15. E2.A5.1.3.4. Omission of material facts was caused or significantly contributed by improper or inadequate advice of authorized personnel, and the previously omitted information was promptly and fully provided;