DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 08-09668
SSN:	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Eric H. Borgstrom, Esquire, Department Counsel
For Applicant: *Pro se*

September 28, 2010

Decision

METZ, John Grattan, Jr., Administrative Judge:

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

On 12 February 2009 the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) to Applicant detailing security concerns under Guidelines M, Use of Information Technology Systems, K, Handling Protected Information, and E, Personal Conduct.[2] Applicant timely answered the SOR, and requested a hearing. DOHA assigned the case to me 2 October 2009, and I convened a hearing 28 October 2009. DOHA received the transcript 3 November 2009.

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

[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 3.c. He is a 37-year-old systems engineer employed by a defense contractor since December 2007. He seeks to retain the security clearance he first obtained while serving in the military.

In 1994, Applicant graduated from a prestigious engineering school with a degree in electrical engineering. In May 1994, he entered the military and served eight years on active duty, and one year in the reserves. He held a clearance and handled classified information without incident while in the service. He married in January 1997 and has two children.

In October 2007, Applicant worked for another defense contractor, physically on-site at the military command that contracted with his company. On 31 October 2007 Applicant installed two unauthorized software programs on his unclassified government computer to bypass the firewall the command had installed to protect the computer system. By so doing, Applicant deliberately violated company regulations, industrial security program regulations, and military agency regulations regarding information technology (IT) systems. Although, Applicant's government computer permitted internet access, the agency firewall blocked access to some sites. Blocked sites included some popular web-based email sites that Applicant wanted to access. He researched the internet for suitable programs, and downloaded two popular freeware programs to bypass the firewall. His system administrator privileges allowed him to install the software.

Applicant used the unauthorized software to tunnel through the agency firewall and access email and other sites that would otherwise have been blocked by the firewall. The software allowed Applicant to access these sites through his home computer. He used the software for several days, usually connecting between his home and work computers when he got to work in the morning, and leaving the connection open all day. According to Applicant, the software was uni-directional—able to connect work to home, but not home to work.

Appellant's unauthorized activity came to light on 7 November 2007, when military IT security personnel detected the tunneling activity between Applicant's work and home computers. They notified Applicant's command of the activity; but, in the meantime, internet connectivity between the command and other organizations was shut down pending investigation of the potential security breach.

In response to a general inquiry begun by Applicant's command, on 8 November 2007 he notified his internet administrator that he had been "pinging" his home computer from his workstation. His workstation was taken off the network. Applicant hoped this would be the end of the incident. When he realized that it would not be, on 9 November 2007 he notified his supervisor that he had also loaded unauthorized software on his work computer. The command suspended Applicant's access on 14

November 2007, and his company fired him on 20 November 2007 because the contract that employed him required him to have access.

Applicant knew his conduct was unauthorized and violated command IT rules, but did it anyway specifically to avoid the firewall. When the tunneling activity was discovered, Applicant deleted one of the programs because he was concerned about its being discovered. Later forensic examination of his work computer showed the two unauthorized programs, but also showed evidence of reformatting that suggested Applicant had acted to remove other incriminating evidence from his computer. The forensic examination concluded that no classified information was on Applicant's work computer.

Applicant's work and character references consider him an outstanding employee who is honest and trustworthy. His current co-workers consider him an excellent employee, and believe he can be trusted with classified information. However, neither of them appears to be aware of the security concerns raised by the Government.

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 adjudicative guidelines should be followed where 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 adjudicative guidelines are Guideline M (Use of Technology Systems), K (Handling Protected Information), and 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. 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.[3]

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

Analysis

The Government established a case for disqualification under Guideline M, and Applicant did not mitigate the security concerns. Applicant deliberately researched the means to avoid the command firewall, deliberately installed those means on his command computer, and then deliberately used those means to access sites the firewall was intended to block.[4] He did this for his personal convenience. His misconduct is recent, did not occur under unusual circumstances or work exigency, and was neither unintentional nor inadvertent. Consequently, none of the mitigating conditions apply.

The Government established case for disqualification under Guideline K, and Applicant did not mitigate the security concerns. Although, the computer system Applicant potentially compromised was the unclassified system at work, the rules Applicant violated were designed to protect the integrity of the computer system as a whole and protect information which, if not classified, was potentially operationally sensitive.[5] Again, Applicant's misconduct is recent, did not occur under unusual circumstances, and was not due to improper or inadequate training. Arguably, Applicant demonstrated the same positive attitude (contemplated by the mitigating factors) toward discharge of security responsibilities before and after the misconduct. Consequently, none of the mitigating conditions apply.

The Government established a case for disqualification under Guideline E, and Applicant did not mitigate the security concerns. When Applicant's breach of the computer system was first discovered, he was not fully candid with government security officials. Not until it became clear that the incident was not going to die down on its own did he disclose the full extent of his misconduct.[6] Although his misconduct was infrequent, it was recent, not minor, and did not occur under unusual circumstances. His misconduct casts doubt on his reliability, trustworthiness, and good judgment, and

---

[4] ¶ 40. (b) illegal or unauthorized modification, destruction, manipulation, or denial of access to information, software, firmware, or hardware in an information technology system; (c) use of any information technology system to gain unauthorized access to another system . . . ; (e) unauthorized use of a government or other information technology system; (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, guidelines, or regulations;

[5] ¶ 34. (g) any failure to comply with rules for the protection of classified or other sensitive information;

[6] ¶ 16. (b) deliberately providing false or misleading information concerning relevant facts to [a] . . . security official . . . or other official government representative; (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. . . ;

despite his claims that he will never do it again, it seems as likely than not that it will. Further, Applicant was over 35 years old when this misconduct began, hardly an age where the conduct might be attributed to youthful indiscretion. I resolve Guideline E against Applicant.

Although this case is alleged under Guidelines M, K, and E, its core is a whole-person analysis. Despite the recommendation of his work and character references, Applicant's poor judgment, unreliability, and untrustworthiness argues against a whole person analysis in his favor. He planned his misconduct and used his technical skill and fiduciary position to execute his misconduct. He did so for his own personal convenience, not for any business or government exigency, and then tried to keep the full extent of his misconduct from government representatives. In effect, Applicant used his position of trust to engage in conduct he was expressly hired to not engage in. He is not suitable for a security clearance.

Formal Findings

Paragraph 1. Guideline M:	AGAINST APPLICANT
Subparagraphs a-c:	Against Applicant
Paragraph 2. Guideline K:	AGAINST APPLICANT
Subparagraph a:	Against Applicant
Paragraph 3. Guideline E:	AGAINST APPLICANT
Subparagraphs a-e:	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