DATE: January 27, 2004

In Re:

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

Applicant for Security Clearance

ISCR Case No. 02-15727

DECISION OF ADMINISTRATIVE JUDGE

ELIZABETH M. MATCHINSKI

APPEARANCES

FOR GOVERNMENT

Rita C. O'Brien, Esq., Department Counsel

FOR APPLICANT

Pro Se

SYNOPSIS

Applicant, a 65-year-old software systems engineer, was terminated from a previous job in July 2002 for violating company policy. He introduced computer software into the company's computer system without authorization, which allowed a third party access to the firm's computer network. Applicant continues to downplay the seriousness of his conduct, characterizing it as "a benign event" since the outside entity only had access to his files. Clearance is denied.

STATEMENT OF CASE

On January 14, 2003, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) to the Applicant which detailed reasons why DOHA could not make the preliminary affirmative finding under the Directive that it is clearly consistent with the national interest to grant or continue a security clearance for the Applicant.(1) DOHA recommended referral to an administrative judge to conduct proceedings and determine whether clearance should be granted, continued, denied, or revoked. The SOR was based on Misuse of Information Technology Systems (Guideline M) and on Personal Conduct (Guideline E) due to his unauthorized installation of a computer software program on his work computer that allowed a third party to gain access to his then employer's computer system.

On February 6, 2003, Applicant filed his response to the SOR allegations and requested a hearing before a DOHA administrative judge. The case was assigned to me on May 6, 2003, and pursuant to formal notice dated May 13, 2003, a hearing was scheduled for June 11, 2003. On May 27, 2003, Applicant requested a continuance of the hearing as the Government intended to offer extracts of his personnel file at his previous job, and his former employer was refusing to release all or part of his personnel file to him. A continuance was granted on June 2, 2003. On receipt of a letter from Applicant indicated he had received information from his personnel file as well as a copy of all releaseable information in his investigative file maintained by the Defense Security Service (DSS), the hearing was rescheduled for September 24, 2003.

At the hearing held as rescheduled, the Government submitted six exhibits and Applicant four exhibits. Testimony was

taken from the Applicant, as reflected in a transcript received October 3, 2003.

FINDINGS OF FACT

The SOR alleged Misuse of Information Technology Systems and Personal Conduct because of the unauthorized introduction of software into his previous employer's computer system in violation of company rules in order to provide a third party access to the company network--conduct for which Applicant was terminated from his employment in July 2000. In his Answer, Applicant admitted he had installed the computer program on his desktop computer, but he denied it was to provide third party access. After a thorough review of the evidence, and on due consideration of the same, I render the following findings of fact:

Applicant is a 65-year-old senior software engineer employed by a defense contractor since September 2000. He held an interim secret clearance from October 18, 2000, and an interim top secret security clearance from May 11, 2001, allowing him to work in a closed area on projects classified to the secret level until clearance was withdrawn on issuance of the SOR.

Applicant has worked as a software engineer in the information technology sector since at least October 1983. After working for nine months as a contract computer programmer analyst at a manufacturing company, Applicant was hired as a permanent employee of the firm in April 1996. In October 1996, Applicant was apprised in writing of the company's external computer access acceptable usage policy, which governed the access from the company's internal network to any non-company host and accessing of the internal network from any external location. Under that policy, employees were specifically advised of the following:

With all external access policies, the basic operating principal is: **'That which is not expressly allowed shall be denied.'** That is, a user must be authenticated and specifically authorized in writing for each service to be accessed externally. All employees utilizing these external services will also adhere to this principle; **if they have not received specific authorization to use a service or perform a function, they are expected to not attempt to access it.** . . .

External access is provided for business purposes only . . .

With external computer access, the availability of obtaining software programs is significantly facilitated. However, introducing software programs into the Company's network via external computer access represents one of the most significant risks to the Company's resources. Therefore, authorization to obtain software in this manner will be severely restricted, requiring specific authorization and strict compliance with approved procedures.

Applicant signed this policy prohibiting him from entering an unauthorized computer software program into the company's computer system.

Applicant's desktop computer at work had password protection capability, but there were occasions where he left his computer unprotected. With the proliferation of inappropriate sites (such as pornography sites) on the Internet, Applicant became concerned in 1998 that another person might use his work computer to gain access to prohibited or illegal sites. Applicant downloaded a computer software program from the Internet designed to monitor his computer's access to the Internet and he installed this program on his work computer. Applicant made no effort to obtain authorization from or even notify his employer of the installation of this software program.[(2)]

For the next two years, this monitoring program ran in the background of his desktop computer at work, recording in a text file the times, dates, and specific websites accessed. Under the terms of the purchase agreement, Applicant was required to provide the outside software company with this data or the program would be shut off.[(3)] For the first six or seven months after the installation, the outside company provided Applicant with a floppy disk on which he downloaded the text file containing the report of his Internet access and mailed the disk back to the company. The company then stopped sending the disk, and even though the program continued to run, Applicant made no effort to inquire about this change in procedure. Without his knowledge, the software company began to upload the data of his Internet access automatically.[(4)]

In Spring 2000, Applicant was transferred to a more sensitive area of the facility where his computer was linked up to the company network computer system in that building. Since his work responsibilities had not changed, Applicant did not give any thought to removing the Internet access monitoring program from his computer, and it continued to run in the background.

During a routine information technology security monitoring of the company network in late June 2000, it was discovered that a third party had access to the company's network. Investigation revealed an outside company had been "pinging" Applicant's desktop through the program he had installed to track his Internet access. Applicant's unauthorized installation and utilization of software on his work computer, which provided a third party with information and potential access to the company's network, was considered to be a serious breach of security. In July 2000, Applicant was involuntarily discharged from the company for violation of company policy regarding the use of company telephone and electronic communications systems. His is not eligible for rehire.

In September 2000, Applicant began working for his current employer, a defense contractor. Needing a security clearance for his duties as a computer software engineer, Applicant executed a security clearance application (SF 86) on September 19, 2000, disclosing that he had been fired from his previous job for installing a computer program on his company-issued computer against company policy. On October 18, 2000, Applicant was granted an interim secret security clearance for his duties.

On April 12, 2001, Applicant was interviewed by a special agent of the Defense Security Service (DSS) about his unauthorized introduction of a software program into his previous employer's computer system. Applicant indicated his intent in installing the monitoring software was to acquire proof should anyone use his computer to access inappropriate sites such as those containing pornography. He expressed his belief that his termination had more to do with his problems with the plant manager rather than his unauthorized introduction of the tracking software into the company's computer system. Applicant explained that when the production software he designed at work developed a glitch, it led to a decline in productivity levels at the plant with a consequent negative impact on the plant manager's work performance. Within a month of this interview, Applicant was granted an interim top secret security clearance.

Applicant has never denied he installed without authorization the Internet access monitoring software onto his work computer in 1998. He denies any company data was ever accessed by the program and from that standpoint, considers it "a benign event." (Tr. 59). Applicant submits he now knows how easily information on a computer that is networked can be illegally accessed if a program that allows external access is installed on the computer, so the probability of him introducing an unauthorized program onto a computer used for national security programs is nonexistent.

Applicant has completed ethics training at his present employment. His work performance evaluations reflect some proficiency in attaining core competencies, as well as significant areas that need improvement.

POLICIES

The adjudication process is based on the whole person concept. All available, reliable information about the person, past and present, favorable and unfavorable, is to be taken into account in reaching a decision as to whether a person is an acceptable security risk. Enclosure 2 to the Directive sets forth adjudicative guidelines which must be carefully considered according to the pertinent criterion in making the overall common sense determination required. Each adjudicative decision must also include an assessment of the nature, extent, and seriousness of the conduct and surrounding circumstances; the frequency and recency of the conduct; the individual's age and maturity at the time of the conduct; the motivation of the individual applicant and extent to which the conduct was negligent, willful, voluntary or undertaken with knowledge of the consequences involved; the absence or presence of rehabilitation and other pertinent behavioral changes; the potential for coercion, exploitation and duress; and the probability that the circumstances or conduct will continue or recur in the future. *See* Directive 5220.6, Section 6.3 and Enc. 2, Section E2.2. Because each security case presents its own unique facts and circumstances, it should not be assumed that the factors exhaust the realm of human experience or that the factors apply equally in every case. Moreover, although adverse information concerning a single guideline may not be sufficient for an unfavorable determination, the individual may be disqualified if available information reflects a recent or recurring pattern of questionable judgment, irresponsibility or emotionally unstable behavior. See Directive, Enc. 2, Section E2.2.4.

Considering the evidence as a whole, the following adjudicative guidelines are the most pertinent to this case:

Guideline M

Misuse of Information Technology Systems

E2.A13.1.1. The Concern: Noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual's trustworthiness, willingness, and ability to properly protect classified systems, networks, and information. Information Technology Systems include all related equipment used for the communication, transmission, processing, manipulation, and storage of classified or sensitive information.

E2.A13.1.2. Conditions that could raise a security concern and may be disqualifying include:

E2.A13.1.2.4. Introduction of hardware, software or media into any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations.

E2.A13.1.3. Conditions that could mitigate security concerns include:

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

Guideline E

Personal Conduct

E2.A5.1.1. The Concern: Conduct involving questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations could indicate that the person may not properly safeguard classified information.

E2.A5.1.2. Conditions that could raise a security concern and may be disqualifying also include:

E2.A5.1.2.1. Reliable, unfavorable information provided by associates, employers. . . .

E2.A5.1.3. Conditions that could mitigate security concerns include:

None.

Under Executive Order 10865 as amended, and the Directive, a decision to grant or continue an applicant's clearance may be made only upon an affirmative finding that to do so is clearly consistent with the national interest. In reaching the fair and impartial overall common sense determination required, the administrative judge can only draw those inferences and conclusions which have a reasonable and logical basis in the evidence of record. In addition, as the trier of fact, the administrative judge must make critical judgments as to the credibility of witnesses. Decisions under the Directive include consideration of the potential as well as the actual risk that an applicant may deliberately or inadvertently fail to properly safeguard classified information.

Burden of Proof

Initially, the Government has the burden of proving any controverted fact(s) alleged in the Statement of Reasons. If the Government meets its burden and establishes conduct cognizable as a security concern under the Directive, the burden of persuasion then shifts to the applicant to present evidence in refutation, extenuation or mitigation sufficient to demonstrate that, despite the existence of conduct raising security concerns, it is clearly consistent with the national interest to grant or continue his security clearance.

A person who seeks access to classified information enters into a fiduciary relationship with the Government predicated upon trust and confidence. Where the facts proven by the Government raise doubts about an applicant's judgment, reliability or trustworthiness, the applicant has a heavy burden of persuasion to demonstrate that he is nonetheless

security worthy. As noted by the United States Supreme Court in *Department of Navy v. Egan*, 484 U.S. 518, 531 (1988), "the clearly consistent standard indicates that security clearance determinations should err, if they must, on the side of denials." Any doubt as to whether access to classified information is clearly consistent with national security will be resolved in favor of the national security.

CONCLUSIONS

Having considered the evidence of record in light of the appropriate legal precepts and factors, and having assessed the credibility of Applicant, I conclude the Government established its case under Guidelines M and E.

Noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual's trustworthiness, willingness and ability to properly protect classified systems, networks, and information. In violation of established company policy regarding computer use and external access, Applicant installed unauthorized software on his desktop computer at his previous place of employment in 1998. He allowed this program to run on the background of his computer for some two years, providing an outside entity access to his employer's computer network even after he was moved to a sensitive area of the facility. Applicant was terminated for what the company considered to be a very serious breach of its security. While Applicant may well have been unaware that the outside company had been "pinging" his computer, he knew he was required to obtain authorization for the installation of any outside software per written company policy he had been apprised of in 1996. He introduced the software on his desktop without making any effort to secure his employer's authorization. Given Applicant's years of experience in the information technology sector and his admitted awareness of the company's policy against accessing pornographic sites, it is simply not credible that he forgot about the specific policy regarding external access. His intentional disregard of known company policy raises very serious security concerns, as set forth under Guideline M (*see* disqualifying condition E2.A13.1.2.4. Introduction of hardware, software or media from any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations), and under Guideline E (*see* E2.A5.1.2.1. Reliable, unfavorable information provided by associates, employers . . .).

Conditions that could mitigate the misuse of information technology systems include: E2.A13.1.3.1. The misuse was not recent or significant; E2.A13.1.3.4. The misuse was an isolated event; and E2.A13.1.3.5. The misuse was followed by a prompt, good faith effort to correct the situation.[(5)] Whereas Applicant provided the avenue whereby an outside entity gained access to the company's computer network, his misuse was clearly significant. Although Applicant installed only one software program, he allowed this unauthorized software to run on his desktop computer for some two years. His misuse of the computer system is regarded as continuing for a substantial period of time until June 2000 and therefore recent and not isolated. While Applicant apparently cooperated with his employer when it was discovered that the outside entity had gained access to the company's computer network, his efforts at rectification come too late for mitigation under E2.A13.1.3.5. Any assumption Applicant might have had that his employer would have overlooked or belatedly accepted the installation of the Internet tracking software based on other employees playing games on their computers at lunchtime would not longer have been reasonable once Applicant was moved to the more sensitive area.

Applicant submits he now knows how easily information on a computer that is networked can be illegally accessed through a program that allows external access, so the probability of him misusing information technology in the future is nonexistent. There is no evidence he has violated his current employer's policies and procedures regarding information technology systems. Yet he still seeks to exonerate his actions at his previous employ by claiming he forgot about the policy that he signed regarding external computer access (Tr. 55) and forgot the tracking program was running on his computer when his office was moved to the secure area (Tr. p. 59). He seeks to minimize the seriousness of his unauthorized installation, characterizing it as a "benign event" since the outside entity did not break into the computer or the network and was just getting one file (Tr. 59), and he downloaded the program in an "open, general area where it really didn't make any difference." (Tr. 61). Applicant's failure to acknowledge or appreciate the significant risks to computer security posed by the introduction of an unauthorized computer program casts significant doubts about his reform.

Apart from the misuse of the computer system itself, there is the issue of his deliberate disregard of company policies that he has inadequately addressed. Whereas Applicant placed his personal interest ahead of his obligation to comply

with his former employer's published policies,[(6)] he has a particularly heavy burden to demonstrate he can be counted on to properly safeguard classified information. His completion of an ethics course at work is not enough to overcome the doubts for his security worthiness, especially where the record is silent as to the nature of the topics covered by the ethics course and where he continues to downplay the risk to security caused by his disregard of policies designed to protect the security of a computer network. Adverse findings are warranted with respect to subparagraphs 1.a. and 2.a. of the SOR.

FORMAL FINDINGS

Formal Findings as required by Section 3. Paragraph 7 of Enclosure 1 to the Directive are hereby rendered as follows:

Paragraph 1. Guideline M: AGAINST THE APPLICANT

Subparagraph 1.a.: Against the Applicant

Paragraph 2. Guideline E: AGAINST THE APPLICANT

Subparagraph 2.a.: Against the 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.

Elizabeth M. Matchinski

Administrative Judge

1. The SOR was issued under Executive Order 10865 (as amended by Executive Orders 10909, 11328, and 12829) and Department of Defense Directive 5220.6 (Directive), dated January 2, 1992 (as amended by Change 4).

2. When interviewed by the Defense Security Service on April 12, 2001, about his unauthorized installation of the software program on his work computer, Applicant claimed that when he installed the program, he completely forgot about the company's policy on external access. (Ex. 2). At his hearing, he attributed his lack of recall of the policy to the fact that half of the software engineers played games which had to be either downloaded or installed by disks that had been purchased. (Tr. 55). Given his concern about someone else accessing an inappropriate site using his computer, it is especially difficult to believe he had forgotten the company policy.

3. Applicant explained the purpose in downloading the information was to alert companies as to who was accessing their website ("It was a like survey." Tr. 50). He initially testified the submission of the data was voluntary (Tr. 51), but later indicated the program would have been shut off if he did not send in the data. (Tr. 52).

4. Applicant claims he forgot about the program and the company. (Tr. 49, 59). While he may well not have known that the company was downloading the data automatically, it is difficult to believe he forgot the program was running on his computer. He has more than twenty years of experience in the computer field.

5. The remaining mitigating conditions under Guideline M do not apply on their face: E2.A.13.1.3.2 The conduct was unintentional or inadvertent (Applicant installed the software for the express purpose of tracking the Internet sites accessed through his desktop computer at work);and E2.A13.1.3.3. The introduction or removal of media was authorized (his firing confirms it was not authorized).

6. Applicant had an alternative in that he could have protected his desktop computer by password. (Tr. 57). His failure to use password protection raises concerns in and of itself about his judgment, reliability and trustworthiness.