DATE: March 12, 2001

In Re:

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

Applicant for Security Clearance

ISCR Case No. 99-0228

APPEAL BOARD DECISION AND REVERSAL ORDER

APPEARANCES

FOR GOVERNMENT

Arthur A. Elkins, Esq., Department Counsel

FOR APPLICANT

Emile J. Henault, Jr., Esq.

Administrative Judge John R. Erck issued a decision, dated August 3, 2000, in which he concluded it is clearly consistent with the national interest to grant or continue a security clearance for Applicant. Department Counsel appealed. For the reasons set forth below, the Board reverses the Administrative Judge's decision.

This Board has jurisdiction on appeal under Executive Order 10865 and Department of Defense Directive 5220.6 (Directive), dated January 2, 1992, as amended.

Department Counsel's appeal presents the following issues: (1) whether the Administrative Judge's findings are supported by substantial record evidence; and (2) whether the Administrative Judge's decision is arbitrary, capricious, or contrary to law.

Procedural History

The Defense Office of Hearings and Appeals issued to Applicant a Statement of Reasons (SOR) dated September 28, 1999. The SOR was based on Guideline M (Misuse of Information Technology) and Guideline E (Personal Conduct).

A hearing was held on May 25, 2000. The Administrative Judge issued a written decision dated August 3, 2000 in which he concluded it is clearly consistent with the national interest to grant or continue a security clearance for Applicant. The case is before the Board on Department Counsel's appeal from the Judge's favorable security clearance decision.

Appeal Issues

1. Whether the Administrative Judge's findings are supported by substantial record evidence. Department Counsel's appeal brief (pp. 10-14) quotes extensive passages from the Administrative Judge's decision and then asserts without elaboration or supporting argumentation that "[t]he record evidence does not support the Administrative Judge's findings of fact." Department Counsel's cursory assertion of factual error lacks specificity. The Board will consider only those claims of factual error that Department Counsel raises with specificity. See ISCR Case No. 99-0295 (October 20, 2000) at pp. 3-4 (explaining why blanket assertions of factual error are inadequate).

Department Counsel specifically contends the record evidence does not support the following findings by the Administrative Judge: (a) Applicant's installation of a Trojan Horse program on a defense agency (hereinafter "Agency") computer system was authorized; (b) Applicant was unaware that his conduct violated Agency rules; and (c) Applicant had never been briefed about the rules, regulations, and guidelines that pertained to Agency computer systems, and he had never seen a copy of the Agency computer security regulations until the hearing.[1]

On appeal, the Board must determine whether "[t]he Administrative Judge's findings of fact are supported by such relevant evidence as a reasonable mind might accept as adequate to support a conclusion in light of all the contrary evidence in the same record. In making this review, the Appeal Board shall give deference to the credibility determinations of the Administrative Judge." Directive, Additional Procedural Guidance, Item E3.1.32.1. The presence of conflicting record evidence does not diminish a Judge's fact-finding responsibility. When the record contains conflicting evidence, the Judge must carefully weigh the evidence in a reasonable, common sense manner and make findings that reflect a reasonable interpretation of the evidence that takes into account all the record evidence. Accordingly, the Board must consider not only whether there is record evidence supporting a Judge's findings, but also whether there is evidence that fairly detracts from the weight of the evidence supporting those findings. *See, e.g.*, ISCR Case No. 99-0205 (October 19, 2000) at p. 2.

The Administrative Judge found: Applicant installed a Trojan Horse program (which captured passwords) on an Agency computer system and transferred the Trojan Horse program to three other Agency work stations; Applicant gained a higher level of access to an Agency computer than he was authorized to by taking advantage of a security vulnerability in the computer system; through these actions, Applicant failed to comply with the rules, procedures, guidelines, or regulations pertaining to the use of Agency information technology systems. Yet, the Judge also found: Applicant had never been informed about the rules, procedures, guidelines, or regulation pertaining to use of Agency computer systems; Applicant did not install the Trojan Horse program to disrupt or sabotage the Agency computer system; Applicant installed the Trojan Horse program to demonstrate a vulnerability in the computer system without knowing that such an installation was prohibited by Agency rules; Applicant gained the higher level of access through the use of an unauthorized procedure in order to assist an Agency system engineer who asked for Applicant's help; Applicant did not obtain root access of the Agency system without authorization; and Applicant did not reconfigure an Agency computer network without authority.

(a) Contrary to Department Counsel's assertion, the Administrative Judge did *not* find that Applicant's actions with respect to installing a Trojan Horse program were authorized. Rather, the Judge appears to have found Applicant's installation of the Trojan Horse program was not authorized, but concluded it was mitigated for various reasons enumerated by the Judge.

(b/c) Department Counsel challenges the Administrative Judge's finding that Applicant was unaware of the rules concerning the proper use of Agency computer systems. Department Counsel's contention has mixed merit. Applicant argues that the Judge's finding is supported by the record evidence and that Department Counsel failed to present evidence rebutting Applicant's explanations for his actions.

Applicant's argument about the absence of evidence rebutting Applicant's explanations is not persuasive. An Administrative Judge is not required to accept testimony merely because it is unrebutted. *See, e.g.*, ISCR Case No. 99-0055 (April 19, 2000) at p. 3. Indeed, it would be arbitrary and capricious for a Judge to uncritically accept a witness's testimony without considering whether it is plausible and consistent with other record evidence. As the Supreme Court noted in *Anderson v. City of Bessemer*, 470 U.S. 564, 575 (1985):

"[T]he trial judge may [not] insulate his findings from review by denominating them credibility determinations, for factors other than demeanor and inflection go into the decision whether or not to believe a witness. Documents or objective evidence may contradict the witness' story; or the story itself may be so internally inconsistent or implausible on its face that a reasonable fact-finder would not credit it. Where such factors are present, the court of appeals may well find clear error even on a finding purportedly based on a credibility determination."

Accordingly, the absence of specific evidence rebutting Applicant's explanations did not compel their acceptance by the Judge.

Department Counsel has the burden of presenting evidence to prove controverted facts. Directive, Additional Procedural Guidance, Item E3.1.14. Absent a showing that the Administrative Judge acted in a manner that is arbitrary, capricious, or contrary to law, the Board will not disturb a Judge's conclusion that Department Counsel failed to satisfy that burden of proof. The Board need not agree with the Judge to conclude Department Counsel has not met its burden of proving the Judge acted in a manner that is arbitrary, capricious, or contrary to law when he concluded Department Counsel failed to prove Applicant had been briefed about the rules, regulations, and guidelines that pertained to Agency computer systems, and Applicant had not seen a copy of the Agency computer security regulations until the hearing.

However, Department Counsel correctly notes there is record evidence that shows Applicant was aware that some of his actions were improper or unauthorized. Even though the Administrative Judge concluded Applicant had not been briefed about the rules, regulations, and guidelines pertaining to Agency computer security, the Judge erred by failing to consider other record evidence relevant to a determination whether Applicant knew or should have known his actions were improper or unauthorized. By repeatedly expressing dissatisfaction with an Agency document and expecting Department Counsel to present the strongest possible evidence (*i.e.*, evidence that Applicant had been formally briefed on computer security), the Judge overlooked relevant record evidence that was probative of Applicant's awareness that his actions were improper and not authorized. *See* ISCR Case No. 95-0817 (February 21, 1997) at pp. 3-4 (Administrative Judge erred by focusing on lack of certain type of evidence the Judge preferred to have and failing to consider other relevant record evidence); DISCR Case No. 93-0059 (March 9, 1994) at p. 4 (Department Counsel not required to present best or strongest possible evidence in order to prove controverted fact); DISCR Case No. 90-1524 (April 29, 1993) at p. 5 n.8 ("However, the fact Department Counsel did not prove the classification status of the materials in question by [a] particular type of evidence does not mean Department Counsel could not prove it by other means.").

To the extent the record evidence shows Applicant was aware his actions were unauthorized, it was arbitrary and capricious for the Administrative Judge to find Applicant was unaware of the rules or proper procedures with respect to those actions. Even in the absence of a formal briefing on computer security, an applicant knows or should know -- through professional training, on the job experience, or common knowledge -- that certain actions violate basic principles of computer security. *Cf.* ISCR Case No. 99-0205 (October 19, 2000) at p. 4 ("It is not plausible for a person who has received an M.B.A. degree to claim to be unaware that the obligation to file state tax returns is separate and independent from the obligation to file federal tax returns, or in the alternative to conclude that such a person would not be knowledgeable enough to be expected to seek proper advice about his or her obligations for filing state tax returns."); ISCR Case No. 98-0265 (March 17, 1999) at p. 7 ("[A]s a matter of common sense, a reasonable employee knows or should know that his or her employer is not paying employees to use company resources and work time to satisfy their sexual desires through pornography, whether it is online or in some other format."); ISCR Case No. 87-2107 (October 25, 1990) at p. 9 ("[A]n applicant's prior training, experience, and current position can be relevant to determining what he or she knows or should know about security regulations, practices and procedures.").[2]

Applicant's acknowledgment that some of his actions were unauthorized could not be ignored or discounted by the Judge, especially in light of the record evidence of Applicant's training and experience with computers and his awareness that certain actions were not consistent with basic principles of computer security.

2. <u>Whether the Administrative Judge's decision is arbitrary, capricious, or contrary to law</u>. Department Counsel contends the Administrative Judge's decision is arbitrary, capricious, and contrary to law because: (a) the record evidence does not support the Judge's conclusion that Applicant's conduct was mitigated; and (b) the Judge failed to articulate a rational basis for his conclusions under Guideline E. Applicant urges affirmance of the Judge's decision on the grounds it reflects a careful and deliberate consideration of all the facts and there is no nexus between the record evidence and Applicant's suitability for a security clearance.

An Administrative Judge's decision can be arbitrary or capricious if: it does not examine relevant evidence; it fails to articulate a satisfactory explanation for its conclusions, including a rational connection between the facts found and the choice made; it does not consider relevant factors; it reflects a clear error of judgment; it fails to consider an important aspect of the case; it offers an explanation for the decision that runs contrary to the record evidence; or it is so implausible that it cannot be ascribed to a mere difference of opinion. *See, e.g.*, ISCR Case No. 99-0154 (December 27, 1999) at p. 3. A Judge is not at liberty to draw whatever inferences or conclusions the Judge wants to. Rather, the Judge

must draw reasonable inferences and reach reasonable conclusions that take into account the totality of the record evidence, evaluate the facts and circumstances of an applicant's case in a manner consistent with the "whole person" analysis required by the Directive, and consider the totality of an applicant's conduct and circumstances under the "clearly consistent with the national interest" standard. *See* ISCR Case No. 99-0511 (December 19, 2000) at pp. 13-14. For the reasons that follow, the Board concludes Department Counsel has demonstrated the Judge's decision is arbitrary and capricious.

(a) The Administrative Judge concluded Applicant's conduct with respect to installing a Trojan Horse program was mitigated because: (i) Applicant had not been informed of the rules, procedures, guidelines, or regulations pertaining to his use of Agency computers; (ii) Applicant did not install the Trojan Horse program to disrupt or sabotage the Agency computer system; (iii) Applicant installed the Trojan Horse program to demonstrate a vulnerability in the Agency computer system; (iv) Applicant's actions were unintentional and inadvertent; (v) there is no evidence that Applicant's actions were undertaken for any malicious or selfish purpose or intent, or that he acted for personal gain or to advance some personal vendetta; (vi) and there is no evidence to refute Applicant's explanation that his action was done in order to enhance the effectiveness of the organization; and (viii) it has been three years since Applicant's conduct occurred without any indication of similar problems in his current assignment. The Judge concluded Applicant's conduct in gaining a higher level of access than he was authorized to have was mitigated because: (i) Applicant had not been informed of the rules, procedures, guidelines, or regulations pertaining to his use of Agency computers; (ii) Applicant did not use the higher level of access for unlawful or sinister purposes; (iii) Applicant used the higher level of access to assist an Agency official who had asked for his assistance; and (iv) it has been three years since Applicant's conduct occurred without any indication of similar problems in his current assignment.

Department Counsel contends the record evidence does not support the Administrative Judge's conclusion that Applicant's conduct was mitigated. In support of this contention, Department Counsel argues the Applicant's explanations about his actions are not conclusive and binding on the Judge, and the Judge failed to consider Applicant's explanations in light of the record evidence as a whole. Department Counsel's contention has merit.

Trojan Horse program. It was arbitrary and capricious for the Administrative Judge to focus on his finding that Applicant had not been briefed about the rules, regulations, and guidelines that pertained to Agency computer systems, and he had not seen a copy of the Agency computer security regulations until the hearing, while ignoring the record evidence that shows Applicant was aware that his conduct was unauthorized. Given Applicant's training and experience with computers, 12 years with the Agency, and his knowledge that the Trojan Horse program would exploit a vulnerability in the Agency computer system, it is untenable for the Judge to find Applicant was unaware that his conduct would violate Agency computer security.

As discussed earlier in this decision, it would be arbitrary and capricious for an Administrative Judge to uncritically accept a witness's testimony without considering whether is plausible and consistent with other record evidence. Accordingly, the Judge erred by finding mitigation based on the absence of evidence to refute Applicant's explanation for why he installed the Trojan Horse program. Furthermore, given the record evidence about the Trojan Horse program and its purpose of capturing passwords, as well as the nature of Applicant's job duties, it is untenable for the Judge to accept as mitigating Applicant's explanation that he merely wanted to demonstrate a vulnerability in the Agency computer system. Even if the Judge had a rational basis to find Applicant did not act out of any sinister, malicious, or unlawful purpose, Applicant's actions in installing the Trojan Horse program were not clearly authorized, reflected poor judgment, and demonstrated a reckless disregard for basic computer security principles. Absent proper authorization to the contrary, any employee (or contractor employee) knows or should know that it is improper to intentionally install malicious software (such as a Trojan Horse program or a computer virus) on a computer, or to deliberately try to capture the computer passwords of other people.

Given the record evidence in this case, it is clear that Applicant deliberately and intentionally installed the Trojan Horse program on the Agency computer system. Accordingly, there is no rational basis for the Administrative Judge to conclude Applicant's conduct was mitigated because it was unintentional and inadvertent.

The record evidence shows that Applicant still believes that he did nothing improper or wrong with respect to his installation of the Trojan Horse program. Given Applicant's inability or unwillingness to recognize or acknowledge that

his conduct was improper and wrong, there is nothing mitigating about the passage of time since Applicant improperly installed the Trojan Horse program on the Agency computer system. *Cf.* ISCR Case No. 96-0360 (September 25, 1997) at p. 5 ("Where an applicant is unwilling or unable to accept responsibility for his or her own actions, such a failure is evidence that detracts from a finding of reform and rehabilitation.").

<u>Gaining higher level access to Agency computer</u>. As discussed earlier in this decision, it was arbitrary and capricious for the Administrative Judge to focus on his finding that Applicant had not been briefed about the rules, regulations, and guidelines that pertained to Agency computer systems, and he had not seen a copy of the Agency computer security regulations until the hearing, while ignoring the record evidence that shows Applicant was aware that his conduct was unauthorized.

The Administrative Judge's finding that Applicant lacked a sinister motive did not make it any less improper for Applicant to gain a higher level access to the Agency computer than he was authorized to have. Clearly, Applicant's motives are a relevant consideration. *See* Directive, Item E2.2.1.7. However, the absence of a sinister motive is not dispositive on whether an applicant's conduct has security significance. *See, e.g.*, ISCR Case No. 99-0454 (October 17, 2000) at p. 6 ("The absence of any sinister motive on Applicant's part does not negate or reduce the negative security significance of his conduct."); DISCR Case No. 90-0998 (December 9, 1992) at p. 6 ("Even without a corrupt or venal motive, an applicant's negligent handling of classified information poses a risk to the national security."). An applicant who recklessly violates basic computer security principles poses a security threat that is not extenuated or mitigated by the absence of a sinister motive.

Furthermore, there is no record evidence that the Agency official who asked for Applicant's assistance had any authority to waive computer security requirements. A reasonable person knows or should know that a request for assistance does not give the requested person *carte blanche* to do anything illegal, improper, or unauthorized when responding to the request for assistance. And, the record evidence shows that Applicant knew his actions would be improper and unauthorized, but he decided to go ahead and do them anyway. Accordingly, the Administrative Judge placed undue weight on his finding that Applicant acted in response to a request for assistance.

The record evidence shows that Applicant still believes that he did nothing improper or wrong with respect to his gaining a higher level of access to the Agency computer than he was authorized to. Given Applicant's inability or unwillingness to recognize or acknowledge that his conduct was improper and wrong, there is nothing mitigating about the passage of time since Applicant improperly gained the higher level of access.

(b) Department Counsel persuasively argues that the Administrative Judge failed to articulate a rational basis for his conclusions under Guideline E. Given the errors demonstrated by Department Counsel, the Judge did not have a rational basis to conclude the government had failed to substantiate its case under Guideline M with respect to his installation of a Trojan Horse program and his gaining a higher level of access to an Agency computer than he was authorized to.[3]

Accordingly, the Judge erred by entering formal findings for Applicant under Guideline E based on his erroneous conclusions under Guideline M.

Moreover, Department Counsel persuasively argues that the Administrative Judge should have analyzed Applicant's conduct under Guideline E independently of his conclusions under Guideline M. An SOR allegation may rationally be included under more than one Guideline. *See, e.g.*, ISCR Case No. 99-0554 (July 24, 2000) at p. 6. Furthermore, a finding of mitigation under one Guideline does not, as a matter of law, compel a finding of mitigation under another Guideline. *See, e.g.*, DISCR Case No. 93-1251 (July 29, 1994) at p. 4. Accordingly, the Judge's finding of mitigation under Guideline M did not relieve the Judge of his obligation to evaluate Applicant's conduct under Guideline E.

Even in the absence of a formal briefing on computer security, Applicant knew or should have known -- through professional training, on the job experience, and common knowledge -- that certain actions he engaged in violated basic principles of computer security. Indeed, the record evidence shows he was aware that his actions were improper and unauthorized. Under the circumstances, Applicant's actions demonstrated poor judgment and reckless disregard for basic principles of computer security. Accordingly, the Judge failed to articulate a rational basis for his favorable conclusions under Guideline E.

Applicant's nexus argument lacks merit. The federal government must be able to repose a high degree of trust and confidence in persons granted access to classified information. *Snepp v. United States*, 444 U.S. 507, 511 n.6 (1980). Security requirements include consideration of a person's judgment, reliability, and trustworthiness. *Cafeteria & Restaurant Workers Union, Local 473 v. McElroy*, 284 F.2d 173, 183 (D.C. Cir. 1960), *aff'd*, 367 U.S. 886 (1961). Persons with access to government computers containing important, sensitive information must be held to high standards of conduct. *See* ADP Case No. 30-1130 (January 4, 2001) at p. 3. Reading the record evidence in a light most favorable to Applicant (the nonappealing party), Applicant's conduct with respect to Agency computers demonstrated poor judgment and a reckless disregard for basic principles of computer security. Applicant's conduct raises serious questions as to his judgment, reliability, and trustworthiness and provides a rational nexus for an adverse security clearance decision.

Conclusion

Department Counsel has met its burden of demonstrating error that warrants reversal. Pursuant to Item E3.1.33.3 of the Directive's Additional Procedural Guidance, the Board reverses the Administrative Judge's August 3, 2000 decision.

Signed: Emilio Jaksetic

Emilio Jaksetic

Administrative Judge

Chairman, Appeal Board

Signed: Michael Y. Ra'anan

Michael Y. Ra'anan

Administrative Judge

Member, Appeal Board

Signed: Jeffrey D. Billett

Jeffrey D. Billett

Administrative Judge

Member, Appeal Board

1. Department Counsel does not specifically challenge the Administrative Judge's findings and conclusions concerning some of the SOR allegations. There is no presumption of error below and the appealing party has the burden of raising and demonstrating error. *See, e.g.*, ISCR Case No. 99-0295 (October 20, 2000) at p. 3. Accordingly, the Board need not address the Judge's findings and conclusions that have not been challenged by Department Counsel.

2. The Board notes that there can be situations where an applicant's conduct "[does] not constitute an obvious, self-evident misuse or unauthorized use of a computer." ISCR Case No. 98-0395 (June 24, 1999) at p. 4. The concept of *res ipsa loquitur* provides a useful analogy. Under the concept of *res ipsa loquitur*, proof of certain facts and circumstances may be give rise to a rebuttable presumption or inference that a person acted negligently. *See, e.g., Black's Law Dictionary* (West Publishing Co., 1990, 6th edition) at p. 1305. However, application of *res ipsa loquitur* would not be appropriate in all cases involving claims of negligence.

3. As discussed in footnote 1, Department Counsel has not challenged the Administrative Judge's findings and conclusions with respect to some of the SOR allegations. Accordingly, the Board need not address whether the Judge had a rational basis for concluding Department Counsel failed to substantiate its case under Guideline M with respect to

those SOR allegations.