DATE: November 27, 2006

---

n re:

---

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

Applicant for Security Clearance

---

CR Case No. 05-09957

**DECISION OF ADMINISTRATIVE JUDGE**

**MARK W. HARVEY**

**APPEARANCES**

**FOR GOVERNMENT**

Julie R. Edmunds, Esq., Department Counsel

**FOR APPLICANT**

*Pro Se*

**SYNOPSIS**

Twenty-eight-year-old Applicant was involved in criminal conduct in 1997, 2001, and 2003. The most serious offenses were in 2001, when he illegally accessed a former employer's computer system, and damaged that system, and in 2003, when he made two false statements on his security clearance application. He failed to mitigate security concerns pertaining to his criminal conduct, personal conduct and misuse of information technology systems. Clearance is denied.

**STATEMENT OF THE CASE**

On November 5, 2003, Applicant applied for a security clearance and submitted a Security Clearance Application (SF 86).[(1)] On February 17, 2006, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) to him, pursuant to Executive Order 10865, *Safeguarding Classified Information Within Industry,* dated February 20, 1960, as amended and modified, and Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (Directive), dated January 2, 1992, as amended and modified.[(2)] The SOR alleges security concerns under Guidelines J (Criminal Conduct), E (Personal Conduct), and M (Misuse of Information Technology Systems). The SOR 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 him, and recommended referral to an administrative judge to determine whether a clearance should be granted, continued, denied, or revoked.

In an answer notarized on April 3, 2006, Applicant responded to the SOR allegations, and elected to have his case decided on the written record in lieu of a hearing.[(3)] A complete copy of the file of relevant material (FORM), dated August 4, 2006, was provided to him on August 11, 2006, and he was afforded an opportunity to file objections and submit material in refutation, extenuation, or mitigation.[(4)] Any such submissions were due by September 10, 2006, but he did not submit any additional information.[(5)] The case was assigned to me on October 12, 2006.

**FINDINGS OF FACT**

As to the factual allegations, Applicant admitted the conduct alleged in the SOR, however, for each SOR allegation he cited possible mitigating circumstances that could reduce security concerns.[(6)] His admissions are incorporated herein as findings of fact. With respect to SOR ¶¶ 1.a, 1.b, and 1.c, he contends the conduct was not recent and his criminal records were expunged. For SOR ¶ 1.d, the conduct was not recent, and he had changed. For SOR ¶¶ 1.e, 2.a, and 2.b, he voluntarily disclosed that he provided inaccurate information on his SF 86. In regard to SOR ¶ 3.a, which alleges the underlying conduct of the criminal conviction alleged in SOR ¶ 1.a, he explained some of the circumstances surrounding his guilty plea to Computer Illegal Access. However, his response to SOR ¶ 1.a contained misleading information about his responsibility for the malicious use of his computer application and his culpability in regard to this offense. This finding is addressed in greater detail in the Findings of Fact, *infra* at 5-6. After a complete and thorough review of the evidence of record, and upon due consideration of the same, I make the following additional findings of fact:

Applicant is 28-years-old.[(7)] He is employed as a software engineer for a defense contractor.[(8)] From 1996 to 2004, he attended college or a university, and was awarded a Master of Science degree.[(9)] Applicant has no prior military service.[(10)] Applicant was married on May 23, 2001.[(11)]

**Criminal Conduct**

SOR ¶¶ 1.a to 1.d, lists four occasions where Applicant was either arrested and/or charged with various violations of state law between 1997 and 2001.[(12)] SOR ¶ 1.e alleges that he violated 18 U.S.C. § 1001 by falsifying two answers on his 2003 SF 86. As indicated previously, he admitted the allegations in SOR ¶ 1.a - 1.d, which lists various charges and some disposition information, but does not detail the underlying circumstances of the conduct. In regard to SOR ¶ 1.a , the investigative report and court records are Items 7 to 9, and provide detailed information about Applicant's conduct. Because SOR ¶ 1.e alleges the same conduct as in SOR ¶¶ 2.a and 2.b, but as a violation of 18 U.S.C. § 1001, SOR ¶ 1.e will be addressed in the Personal Conduct section, *infra*.

On September 10, 1997, Applicant was charged with Dishonesty, Theft, Vandalism, and Failure to Comply (SOR ¶ 1.d). He was fined $50.00, assigned to alcohol education, and relocated to another residence on campus. He received probation before judgment and his criminal record was subsequently expunged.

On December 13, 1998, he was arrested for 3rd Degree Burglary, 2nd Degree Assault, Giving a False Fire Alarm, Malicious Destruction of Property and Petty Theft (SOR ¶ 1.c). Applicant states the entire incident was a big misunderstanding, and it was placed on the "stet" docket. This conviction was subsequently expunged.[(13)]

On August 11, 2000, he was arrested for Driving Under the Influence of Alcohol (DUI) (SOR ¶ 1.b). On November 17, 2000, he received probation before judgment, and his driver's license was suspended for 45 days.

On February 20, 2001, he was arrested for Computer/Illegal Access/Damage (SOR ¶ 1.a). On March 22, 2001, he pleaded guilty to Computer Illegal Access. The court sentenced him to 80 hours of community service, probation for 12 months, a fine and court costs of $250.00, and restitution of $5,187.00. He was also required to receive psychological counseling. On June 23, 2005, the court issued an order expunging the police and court records concerning this incident.[(14)] The facts pertaining to this offense are discussed at pages 5-6, *infra*.

**Personal Conduct**

The evidence of record establishes Applicant's knowing and deliberate falsification as alleged in SOR ¶¶ 2.a and 2.b of Questions 6 and 26, respectively of Applicant's October 29, 2003, security clearance application.

Question 6 asks about his employment activities. He falsely stated that he was unemployed from February 1999 to December 1999, when he was actually employed with an organization (DT) that subsequently accused him of deliberately damaging their computer system. Applicant said he omitted employment information concerning DT because he "did not think [the employer] was still in business. Before submitting my SF-86, I drove by the location that

I worked at . . . and they were no longer there."[(15)] He said he subsequently brought this omission to the attention of the DSS interviewer, and previously listed this information on his SF-85P back in 2001.[(16)] Question 26 refers to "Your Police Record - Other Offenses," and asks:

In the last 7 years, have you been arrested for, charged with, or convicted of any offense(s) not listed in modules 21, 22, 23, 24, or 25? (Leave out traffic fines of less than $150 unless the violation was alcohol or drug related.) For this item, report information regardless of whether the record in your case has been sealed or otherwise stricken from the record. The single exception to this requirement is for certain convictions under the Federal Controlled Substances Act for which the court issued an expungement order under the authority 21 U.S.C. 844 or 18 U.S.C. 3607.

Applicant responded, "Yes."[(17)] and listed a December 1, 1998, Destruction of Property offense, the particular court where the case was adjudicated and the court's location, as well as the current status of the record as expunged.[(18)] In his response to the SOR Applicant asserts he made a prompt, good faith effort to correct the falsification before being confronted with the facts, and he explains his incorrect answer:

company security started making urgent requests to submit my SF-86 paperwork. Due to the urgency, I overlooked this since I did not have the case number, court date, and the official name of the charges. I corrected this by bringing this information directly to [the attention of the DSS agent on December 17, 2004] before my subject interview began.[(19)]

Question 26 does not seek and Applicant did not provide the case number or the court date pertaining to his December 1, 1998, Destruction of Property offense. The most significant criminal offense that was not included on his 2003 SF 86 was the March 22, 2001, conviction for Computer Illegal Access, which is discussed in greater detail in the next section, *infra*.

SOR ¶ 1.e alleges the same conduct as alleged in SOR ¶¶ 2.a and 2.b, but as a violation of 18 U.S.C. § 1001. Neither of Applicant's explanations for the two omissions to his 2003 SF 86 are credible. I infer that he did not list his employment with DT or his 2001 conviction because he wanted to conceal the facts surrounding his 2001 conviction for Computer Illegal Access. These two omissions are material, and deliberate and as such his conduct constitutes a violation of 18 U.S.C. § 1001.

**Misuse of Information Technology Systems**

DT sought the assistance of the police because DT was receiving numerous spam emails, some including profanity, in sufficient volume to shut down DT's computer system.[(20)] Applicant had previously left DT's employment on "bad terms."[(21)] DT suggested to the police that Applicant might be responsible for the emails.[(22)] On January 12, 2001, he admitted to the police that he was responsible for spamming DT.[(23)] While employed at DT, he placed a file on DT's website without DT's permission so that he could access DT's website after his employment terminated.[(24)] He subsequently accessed DT's website without DT's permission.[(25)]

DT provided to the court documentation showing Applicant's misconduct required 84 hours of labor by six of DT's employees, to track down the source of the problem, communicate with police, clean the spam off computers, and move their website to a new server.[(26)] Applicant paid DT court ordered restitution of $5,186.59 as part of his sentence for Computer Illegal Access.

In Applicant's response to the SOR, notarized on April 3, 2006, he explained this offense as follows:

Back in 1999, e-commerce was beginning to evolve and I developed a simple email application. This simple application was developed to see what capabilities that email can do, which just consisted of a web page to enter: to, from subject, and message body information of an email. At the time, I was in college working on my undergraduate degree. Since this was one of my very first software programs, I showed it to several classmates and to my wife's friends. If I had known at the time it would've been used in a malicious manner, I would have disposed of this program. Unfortunately, I was unaware of this [un]til I was charged in reference to subparagraph 1.a [of the SOR].

Applicant's response to the SOR is deliberately misleading. It does not admit that he personally, and deliberately placed his application on DT's website and then maliciously used his application or spamming to damage DT's computer system. Instead he implies that someone else misused his application, and does not address his spamming of DT's computer network.

## POLICIES

In an evaluation of an applicant's security suitability, an administrative judge must consider Enclosure 2 of the Directive, which sets forth adjudicative guidelines. In addition to brief introductory explanations for each guideline, the adjudicative guidelines are divided into Disqualifying Conditions (DC) and Mitigating Conditions (MC), which are used to determine an applicant's eligibility for access to classified information.

These adjudicative guidelines are not inflexible ironclad rules of law. Instead, recognizing the complexities of human behavior, an administrative judge should apply these guidelines in conjunction with the factors listed in the adjudicative process provision in Section E2.2, Enclosure 2, of the Directive. An administrative judge's overarching adjudicative goal is a fair, impartial and common sense decision.Because the entire process is a conscientious scrutiny of a number of variables known as the "whole person concept," an administrative judge should consider all available, reliable information about the person, past and present, favorable and unfavorable, in making a meaningful decision.

Specifically, an administrative judge should consider the nine adjudicative process factors listed at Directive ¶ E2.2.1: (1) the nature, extent, and seriousness of the conduct; (2) the circumstances surrounding the conduct, to include knowledgeable participation; (3) the frequency and recency of the conduct; (4) the individual's age and maturity at the time of the conduct; (5) the voluntariness of participation; (6) the presence or absence of rehabilitation and other pertinent behavioral changes; (7) the motivation for the conduct; (8) the potential for pressure, coercion, exploitation, or duress; and (9) the likelihood of continuation or recurrence.

Based upon a consideration of the evidence as a whole, I find the following adjudicative guidelines most pertinent to an evaluation of the facts of this case:

**Criminal Conduct - Guideline J: "A history or pattern of criminal activity creates doubt about a person's judgment, reliability and trustworthiness." Directive ¶ E2.A10.1.1.**

**Personal Conduct - Guideline E: "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." Directive ¶ E2.A5.1.1.**

**Misuse of Information Technology Systems - Guideline M: "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." Directive ¶ E2.A13.1.1.**

Conditions that could raise a security concern and may be disqualifying, as well as those which could mitigate security concerns, pertaining to these three adjudicative guidelines are set forth and discussed in the Conclusions section below.

Since the protection of the national security is the paramount consideration, the final decision in each case is arrived at by applying the standard that the issuance of the clearance is "clearly consistent with the interests of national security." In reaching this decision, I have drawn only those conclusions that are reasonable, logical and based on the evidence contained in the record. Likewise, I have avoided drawing inferences grounded on mere speculation or conjecture.

In the decision-making process, facts must be established by "substantial evidence.[(27)] The government initially has the burden of producing evidence to establish a case which demonstrates, in accordance with the Directive, that it is not clearly consistent with the national interest to grant or continue an applicant's access to classified information. Once the government has produced substantial evidence of a disqualifying condition, the burden shifts to Applicant to produce

evidence and prove a mitigating condition. Directive ¶ E3.1.15 provides, "The applicant is responsible for presenting witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by applicant or proven by Department Counsel, and [applicant] has the ultimate burden of persuasion as to obtaining a favorable clearance decision." The burden of disproving a mitigating condition never shifts to the government. *See* ISCR Case No. 02-31154 at 5 (App. Bd. Sep. 22, 2005).[(28)]

A person who seeks access to classified information enters into a fiduciary relationship with the government predicated upon trust and confidence. It is a relationship that transcends normal duty hours and endures throughout off-duty hours as well. It is because of this special relationship the government must be able to repose a high degree of trust and confidence in those individuals to whom it grants access to classified information. Decisions under this Directive include, by necessity, consideration of the possible risk an applicant may deliberately or inadvertently fail to protect or safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation as to potential, rather than actual, risk of compromise of classified information.

The scope of an administrative judge's decision is limited. Applicant's allegiance, loyalty, and patriotism are not at issue in these proceedings. Section 7 of Executive Order 10865 specifically provides industrial security clearance decisions shall be "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." Security clearance decisions cover many characteristics of an applicant other than allegiance, loyalty, and patriotism. Nothing in this Decision should be construed to suggest that I have based this decision, in whole or in part, on any express or implied determination as to Applicant's allegiance, loyalty, or patriotism.

## CONCLUSIONS

Upon consideration of all the facts in evidence, and after application of all appropriate legal precepts, factors, and conditions, including those described briefly above, I conclude the following with respect to the allegations set forth in the SOR:

**Criminal Conduct**Under Guideline J, a history or pattern of criminal activity raises questions regarding an applicant's willingness or ability to protect classified information and creates doubt about a person's judgment, reliability and trustworthiness. Directive ¶ E2.A10.1.1.

Two criminal conduct disqualifying conditions (CC DC) could raise a security concern in this case. CC DC 1 applies where there are "[a]llegations or admissions of criminal conduct, regardless of whether the person was formally charged" and CC DC 2 applies in situations where an applicant has committed "a single serious crime or multiple lesser offenses." Directive ¶¶ E2.A10.1.2.1 and E2.A10.1.2.2. CC DC 1 and 2 apply because Applicant committed multiple criminal offenses (SOR ¶¶ 1.a, 1.d, and 1.e.), and one of the three offenses is a serious crime (SOR ¶ 1.e alleges a violation of 18 USC §1001, which is a felony). In regard to the allegations in SOR ¶¶ 1.b and 1.c, I conclude that these two incidents are not established by substantial evidence.

Security concerns based on criminal conduct can be mitigated by showing that it was not recent (CC MC 1). Directive ¶ E2.A10.1.3.1. There are no "bright line" rules for determining when conduct is "recent." The determination must be based "on a careful evaluation of the totality of the record within the parameters set by the directive." ISCR Case No. 02-24452 at 6 (App. Bd. Aug. 4, 2004). If the evidence shows "a significant period of time has passed without any evidence of misconduct," then an administrative judge must determine whether that period of time demonstrates "changed circumstances or conduct sufficient to warrant a finding of reform or rehabilitation." *Id*. CC MC 1 does not apply because Applicant's last incident of criminal conduct was his false statement, when he filled out his security clearance application on October 29, 2003. Moreover, he was not forthright and candid when addressing his culpability in relation to Computer Illegal Access (SOR ¶ 1.a) in his response to the SOR, dated March 14, 2006.[(29)], [(30)]

Criminal conduct security concerns may be mitigated under CC MC 2 when the "crime was an isolated incident," Directive ¶ E2.A10.1.3.2, or under CC MC 3 when an applicant demonstrates he "was pressured or coerced into committing the act and those pressures are no longer present in that person's life." Directive ¶ E2.A10.1.3.3. CC MCs 2 and 3 do not apply because Applicant committed three criminal offenses, and no one caused him or influenced him to commit the criminal conduct.

For CC MC 4, security concerns pertaining to criminal conduct may be mitigated when an applicant "did not voluntarily commit the act and/or the factors leading to the violation are not likely to recur." Directive ¶ E2.A10.1.3.4. Applicant voluntarily committed the criminal conduct, and has not shown a sufficient track record of positive or non-criminal conduct. CC MC 4 does not apply.

In regard to CC MCs 5 and 6, security concerns may be mitigated when an applicant was acquitted or "[t]here is clear evidence of successful rehabilitation." Directive ¶¶ E2.A10.1.3.5 and E2.A10.1.3.6. CC MC 5 and 6 do not apply because in regard to SOR ¶¶ 1.a, 1.d, and 1.e, Applicant was not acquitted and there is a dearth of evidence about changes in his life that establish his rehabilitation.

**Personal Conduct**

Under Guideline E, "conduct involving questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations could indicate that applicant may not properly safeguard classified information." Directive ¶ E2.A5.l.l.

Three personal conduct disqualifying conditions (PC DC) could potentially raise a security concern and may be disqualifying in this case. PC DC 2 applies where there has been "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, determine employment qualifications, award benefits or status, determine security clearance eligibility or trustworthiness, or award fiduciary responsibilities." Directive ¶ E2.A5.1.2.2. A security concern may result under PC DC 3 when an applicant deliberately provides "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." Directive ¶ E2.A5.1.2.3. PC DC 5 applies when an applicant has "a pattern of dishonesty or rule violations." Directive ¶ E2.A5.1.2.5.

For SOR ¶ 2.a, Applicant's response to the SOR establishes PC DCs 2 and 3 by substantial evidence. He deliberately gave a false answer to Questions 6 and 26 of his security questionnaire on October 29, 2003, in an attempt to conceal his malicious damage to his former employer's computer system. The evidence of record establishes SOR ¶¶ 2.a and 2.b by substantial evidence because he admits preparing his security questionnaire, that he understood the questions, and that he provided answers that omitted important information. The omitted information would have provided or led the government to material derogatory information. PC DC 5 does not apply to SOR ¶¶ 2.a and 2.c because the falsification occurred on the same 2003 SF 86.

A security concern based on Guideline E may be mitigated by substantial evidence of personal conduct mitigating conditions (PC MC). Under PC MC 1, security concerns may be mitigated when the derogatory "information was unsubstantiated or not pertinent to a determination of judgment, trustworthiness, or reliability." Directive ¶ E2.A5.1.3.1. The allegations in SOR ¶¶ 2.a and 2.b are established by substantial evidence, and constitute deliberate falsifications. As such SOR ¶¶ 2.a and 2.b are relevant to making a security determination about his judgment, trustworthiness, and reliability.

PC MC 2 applies when the "falsification was an isolated incident, was not recent, and the individual has subsequently provided correct information voluntarily." Directive ¶ E2.A5.1.3.2. PC MC 3 applies when the "individual made prompt, good-faith efforts to correct the falsification before being confronted with the facts." Directive ¶ E2.A5.1.3.3. Applicant has partially established PC MCs 2 and 3 because only two falsifications are established, and they both occurred on the same security clearance application on October 29, 2003, over three years ago. Additionally, he made a belated, good-faith effort to correct the record when he disclosed the falsification in 2004 to a DSS investigator. Although his eventual admission that the clearance entry was false was not "prompt," he deserves some credit under the "whole person" concept for eventually providing accurate information. *See* ISCR Case No. 04-07360 at 2, 3 (App. Bd. Sep. 26, 2006) (indicating when a mitigating condition cannot be fully applied, "some credit" is still available under that same mitigating condition).

PC MC 4 applies when "[o]mission of material facts was caused or significantly contributed to by improper or inadequate advice of authorized personnel, and the previously omitted information was promptly and fully provided." Directive ¶ E2.A5.1.3.4. There is no evidence that anyone gave Applicant improper or inadequate advice or suggested

that he omit information from his SF-86. Security concerns can be mitigated under PC MC 5 when an applicant "has taken positive steps to significantly reduce or eliminate vulnerability to coercion, exploitation, or duress." Directive ¶ E2.A5.1.3.5. Under PC MC 5, Applicant receives some credit for eventually disclosing his 2001 conviction and his employment by DT, but PC MC 5 may not be fully applied because his response to the SOR substantially understated his role in the 2001 Computer Illegal Access (SOR ¶ 1.a). His steps made toward rehabilitation are insufficient in magnitude and too recent to support full application of PC C 5.

In sum, Applicant's October 29, 2003, false statements about his prior conviction and employment with DT reflect questionable judgment, untrustworthiness, and dishonesty. Standing individually, they might be regarded as isolated, minor offenses that are somewhat remote in time. Directive ¶¶ 6.3.1 and 6.3.2. However, taken together, along with his criminal conduct and misleading response to the SOR, his personal conduct is not mitigated.

**Misuse of Information Technology Systems**

Under Guideline M, "[n]oncompliance 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." Directive ¶ E2.A13.1.1.

There are four potential information technology disqualifying conditions (IT DC) that could raise a security concern, but only two may be disqualifying in this case. IT DC 1 applies where there has been "[i]llegal or unauthorized entry into any information technology system." Directive ¶ E2.A13.1.2.1. IT DC 2 applies where an applicant engages in "[i]llegal or unauthorized modification, destruction, manipulation, or denial of access to information residing on an information technology system." Directive ¶ E2.A13.1.2.2. IT DC 3 applies where an applicant removes or uses "hardware, software or media from any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations." Directive ¶ E2.A13.1.2.3. IT DC 4 applies where an applicant introduces "hardware, software or media into any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations." Directive ¶ E2.A13.1.2.4.

IT DC 1 applies because Applicant illegally and without authorization entered DT's computer system after his employment was terminated. IT DC 2 applies because he sent so much span to DT's computer system that DT's computer system had to be shut down, temporarily denying access to users. IT DC 3 and 4 do not apply because the record does not contain any "rules, procedures, guidelines or regulations" that were violated.

A security concern based on Guideline M may be mitigated by substantial evidence of any of five IT mitigating conditions (IT MC). Under IT MC 1, security concerns may be mitigated when the "misuse was not recent or significant." Directive ¶ E2.A13.1.3.1. IT MC 2 applies when the "conduct was unintentional or inadvertent." Directive ¶ E2.A13.1.3.2. IT MC 3 applies when the "introduction or removal of media was authorized." Directive ¶ E2.A13.1.3.3. IT MCs 4 or 5 applies when the misuse was "an isolated event" or "followed by a prompt, good faith effort to correct the situation." Directive ¶¶ E2.A13.1.3.4 and E2.A13.1.3.5.

The allegations in SOR ¶ 3.1 are not mitigated. His 2001 damage to DT's computer system cannot be considered in isolation or in a piecemeal fashion. In the context of his other misconduct, his 2001 Computer Illegal Access is sufficiently recent, significant and not isolated to bar application of IT MCs 1 and 4. The 2001 Computer Illegal Access was intentional, deliberate, unauthorized, and not disclosed by Applicant in time to avoid damage to DT's computer system, and IT MCs 2 and 3 are not applicable.

**"Whole Person" Analysis**

In addition to the enumerated disqualifying and mitigating conditions as discussed previously, I have considered the general adjudicative guidelines related to the whole person concept under Directive provision E2.2.1. As noted above, Applicant's history of criminal conduct, is counterbalanced by his change in circumstances-he indicates marriage, graduation and post-DT employment have improved his decision-making process. E2.2.1.1. His actions concerning criminal conduct, especially the falsification of his 2003 security clearance application, and his 2001 damage to DT's computer system were knowledgeable and voluntary. E2.2.1.2. He was in his early 20's when he damaged DT's computer system, and falsified his SF 86. A person in their early 20's is sufficiently mature to be fully responsible for

their conduct. E2.2.1.4. The likelihood of future criminal conduct and falsifications remains substantial because such a short period of time has elapsed since his last false or misleading statement (response to SOR on March 14, 2006), and he has not provided sufficient evidence of a change in his lifestyle. E2.2.1.9. His relative youth, and achievement of a Master's Degree provide some mitigation, but the possibility remains of compromise of sensitive or classified information. His failure to provide a credible description of his damage to DT's computer system in his response to the SOR weighs heavily against him. After weighing the disqualifying and mitigating conditions, all the facts and circumstances, in the context of the whole person, I conclude Applicant has not mitigated the security concerns pertaining to criminal conduct, personal conduct, and misuse of information technology systems.

The evidence leaves me with grave questions and doubts as to Applicant's security eligibility and suitability. I take this position based on the law, as set forth in *Department of Navy v. Egan,* 484 U.S. 518 (1988), my "careful consideration of the whole person factors"[(31)] and supporting evidence, my application of the pertinent factors under the Adjudicative Process, and my interpretation of my responsibilities under Enclosure 2 of the Directive. Applicant has failed to mitigate or overcome the government's case. I conclude Applicant is not eligible for access to classified information.

## FORMAL FINDINGS

Formal findings For or Against Applicant on the allegations set forth in the SOR, as required by Section E3.1.25 of Enclosure 3 of the Directive, are:

Paragraph 1, Guideline J: AGAINST APPLICANT

Subparagraph 1.a: Against Applicant

Subparagraph 1.b: For Applicant

Subparagraph 1.c: For Applicant

Subparagraph 1.d: Against Applicant

Subparagraph 1.e: Against Applicant

Paragraph 2, Guideline E: AGAINST APPLICANT

Subparagraph 2.a: Against Applicant

Subparagraph 2.b: Against Applicant

Paragraph 3, Guideline M: AGAINST APPLICANT

Subparagraph 3.a: 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 is denied.

Mark W. Harvey

Administrative Judge

1. Item 4, Electronic Standard Form (SF) 86, Security Clearance Application is dated November 5, 2003, on the first page. The first page also indicated Applicant signed the SF 86 on October 29, 2003. There is an allegation of falsification of this SF 86 in SOR ¶¶ 2.a and 2.b.

2. Item 1 (Statement of Reasons (SOR), dated February 17, 2006) at 1-3. Item 1 is the source for the remainder of this paragraph.

3. Item 3, Applicant's response to SOR is dated March 14, 2006, and notarized on April 3, 2006.

4. The Defense Office of Hearings and Appeals (DOHA) transmittal letter is dated August 9, 2006. It was served on Applicant on August 11, 2006.

5. *Id*. The DOHA transmittal letter informed Applicant that he had 30 days after receipt to submit information.

6. Item 3, *supra* note 3, is the source for all factual assertions in this paragraph.

7. Item 4, *supra* note 1, section 1.1, at 1.

8. *Id.*, section 6.1, at 3.

9. *Id*., section 5, at 2-3, and Item 3, *supra* note 3, at 1.

10. Item 4, *supra* note 1, section 11, at 5.

11. *Id.*, section 8, at 4-5.

12. Unless otherwise noted in the body of the paragraph or in a footnote, Items 1 (SOR) and 3 (Response to SOR) are the sources for the facts in this section.

13. *See* note 18, *infra*.

14. Item 3, *supra* note 3, at 8-13 (expungement documentation).

15. *Id*. at 2-3.

16. A copy of his 2001 SF-85P is not part of the record evidence.

17. Item 4, section 26, at 7-8.

18. Item 6, at 2, is a screen shot indicating an offense date of December 1, 1998, an offense of "Destruction of Property," and Action Taken, "Record Expunged." This offense is apparently the one involving the arrest on December 13, 1998 (SOR ¶ 1.c).

19. Item 3, *supra* note 3, at 3, and Item 5 (responses to interrogatories) at 5.

20. Item 7 at 1-2 and Item 8 at 2.

21. Item 7 at 2. Applicant indicated he left DT's employment because of a timecard dispute. The police reports do not elaborate or provide additional details about why he left DT's employment.

22. *Id*. at 3-6.

23. *Id*. at 5.

24. Item 8, at 3.

25. The connection between the spamming and Applicant's placement and post-employment use of his access to DT's web site is not explained in the police report.

26. Item 9 at 5.

27. "Substantial evidence [is] such relevant evidence as a reasonable mind might accept as adequate to support a conclusion in light of all the contrary evidence in the record." ISCR Case No. 04-11463 at 2 (App. Bd. Aug. 4, 2006) (citing Directive ¶ E3.1.32.1). "This is something less than the weight of the evidence, and the possibility of drawing two inconsistent conclusions from the evidence does not prevent [a Judge's] finding from being supported by substantial evidence." *Consolo v. Federal Maritime Comm'n*, 383 U.S. 607, 620 (1966). "Substantial evidence" is "more than a scintilla but less than a preponderance." *See v.Washington Metro. Area Transit Auth*., 36 F.3d 375, 380 (4th Cir. 1994).

28. "The Administrative Judge [] consider[s] the record evidence as a whole, both favorable and unfavorable, evaluate[s] Applicant's past and current circumstances in light of pertinent provisions of the Directive, and decide[s] whether Applicant ha[s] met his burden of persuasion under Directive ¶ E3.1.15." ISCR Case No. 04-10340 at 2 (App. Bd. July 6, 2006).

29. See Item 3, *supra* note 3, at 1 (addressing SOR ¶ 1.a), and pages 5-6 of this decision, *supra*.

30. "Conduct not alleged in a SOR may be considered: (a) to assess an applicant's credibility; (b) to evaluate an applicant's evidence of extenuation, mitigation, or changed circumstances; (c) to consider whether an applicant has demonstrated successful rehabilitation; (d) to decide whether a particular provision of the Adjudicative Guidelines is applicable; or (e) to provide evidence for whole person analysis under Directive Section 6.3." ISCR Case No. 03-20327 at 3 (App. Bd. Oct. 26, 2006) (citing ISCR Case No. 00-0633 at 3 (App. Bd. Oct. 24, 2003)).

31. *See* ISCR Case No. 04-06242 at 2 (App. Bd. June 28, 2006).