DEPARTMENT OF DEFENSE
DEFENSE LEGAL SERVICES AGENCY
DEFENSE OFFICE OF HEARINGS AND APPEALS
WASHINGTON HEARING OFFICE
POST OFFICE BOX 3627
ARLINGTON, VIRGINIA 22203-1995
FAX (703) 696-1831

DATE: MAY 17

In Re:	)	
STEELE, Robert David SSN: 213-72-2838	)	ISCR Case No. 02-22067
Applicant for Security Clearance	)	

DECISION OF ADMINISTRATIVE JUDGE
PAUL J. MASON

APPEARANCES

FOR GOVERNMENT
Robert E. Coucher, Esq., Department Counsel

FOR APPLICANT
Phillip D. Cave, Esq.

SYNOPSIS

Applicant's employment activities relating to open source intelligence (conducting conferences and delivering presentations/training sessions) do not pose a conflict with his security clearance responsibilities to his defense contractor or the United States military agencies. While Applicant's business reputation and his achievements in the open source intelligence domain are commendable, his deliberate falsifications of two security clearance applications have not been mitigated. Clearance is denied.

STATEMENT OF CASE

On October 29, 2004, the Defense Office of Hearings and Appeals (DOHA), pursuant to Department of Defense Directive 5220.6, dated January 2, 1992, as reissued through Change 4 thereto, dated April 20, 1999, 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 Applicant. DOHA recommended referral to an Administrative Judge to conduct proceedings and determine whether clearance should be granted, continued, denied or revoked. On January 24, 2005, Applicant provided his response to the SOR and requested a hearing before an Administrative Judge.

The case was assigned to me on October 26, 2005. On October 20, 2005, this case was set for hearing on November 9, 2005. The Government submitted six exhibits, and Applicant submitted two exhibits. Testimony was taken from Applicant. At the conclusion of the hearing, Applicant was given 14 days to submit documentation. Applicant furnished AE C on November 15, 2005. On November 22, 2002, Department Counsel noted the documentation within AE C identified a problem in the relationship between the United States (U.S.) Agency 1 and Appellant's company (Company C) because neither Applicant's company nor Applicant has a facility security clearance, and Applicant's personal security clearance is authorized only when he is performing consulting services for his defense contractor. The transcript (Tr.) was received on November 23, 2005.

Applicant submitted AE D on January 29, 2006. On February 7, 2006, Department Counsel objected to AE D as being beyond the 14-day period allowed for post hearing submissions. In order to allow for the development of a full record, Department Counsel's objection is overruled. AE C and AE D have been admitted in evidence.

FINDINGS OF FACT

The SOR alleges outside employment activities (Guideline L), personal conduct (Guideline E), and criminal conduct (Guideline J). Applicant essentially admitted the factual allegations under the outside activities guideline but denied those activities pose a conflict with his security responsibilities or increased the risk of unauthorized disclosure of classified information. He also denied the personal conduct and criminal conduct allegations.

Applicant's Background. Applicant was born in State 1 in July 1952. In 1974, he received his Bachelor of Arts degree in political science. In 1976, he received a Master's degree in international relations. From June 1976 to December 1979, Applicant served as an officer in the United States Agency 3 where he was assigned to infantry leadership and administrative management. According to his security clearance application (SCA) dated April 2004, from 1979 to 1993, Applicant was employed in intelligence positions for Agency 3 and Agency 4.

After Applicant was informed in April 1993 he could not conduct open source intelligence activity inside the federal government, he founded Company A, and became chief executive officer. In June 1997, Applicant changed the name of the company to Company B. In June 2003, Applicant renamed his company again to Company C. As the principal officer of Company C (and predecessor

companies), his primary objective has been the collection and exploitation of open sources of information through legal avenues for the United States military. The official title of the intelligence gathering process (in existence since about 1988) is open source intelligence, defined by Applicant as follows:

> Open source intelligence is the discovery, discrimination, distillation, and dissemination of print, audio, image, and interview information that can be obtained legally and ethically, in any language. OSINT (open source intelligence) by definition cannot violate any law or confidence, and in no way, shape, or form associated with espionage, secret activities, or concealed relationships. Examples of open source intelligence include Internet searching, media and published journal research, gray literature acquisition (telephone books, university yearbooks), and an expert interview or subcontracting (GE 3).

Applicant has applied the intelligence gathering methodologies to the world of open source intelligence (Tr. 37). He uses his website (Company C) to enhance his credibility when identifying and engaging the appropriate expertise to resolve tasks of the U.S. Agency 1. Applicant is employed primarily by the U.S. Agency 1 with a Top Secret clearance so that he can train individuals in open source intelligence. Applicant also manages an annual conference in Washington, D.C. that has trained about 7,500 intelligence professionals since he founded the company in 1993. Applicant also periodically conducts a one-day training course in open source intelligence to the U.S. Government and to foreign governments.

Applicant has authored books and delivered speeches on open source intelligence and intelligence reform (GE 3). He has been a guest lecturer at military schools and various security and military conferences. Applicant has continuously held a Top Secret security clearance since 1976 when he joined Agency 3 (Tr. 29). During the period, he has committed only three security violations while on active duty between 1976 and 1979 (*Id.*).

Outside Activities (Guideline L). As stated in subparagraph 1.a. of the SOR, Applicant was the primary owner and manager of Company B, and is currently the owner of Company C, however, he has never been involved in "all-source endeavors." His only business is open source intelligence. Applicant's company, Company C, has provided services on unclassified contracts to U.S. Agency 1, three trans Atlantic agencies. (subparagraph 1.b.). Applicant has provided services related to open source intelligence since 1993. Applicant manages a conference in Washington, D.C. (subparagraph 1.c.) that trains the U.S. military, U.S. civilian intelligence professionals, and foreign civilian and military intelligence professionals. The conference was not held in 2005 due to Applicant's other commitments. Applicant has managed over 15 international conferences and trained over 5,000 intelligence professionals in open source intelligence (subparagraph 1.d.).

As alleged in subparagraph 1.e.(1), and as Applicant stated in GE 3 (sworn statement dated June 25, 2003), he has trained and coached several members of foreign intelligence training organizations stated in GE 3. However, his training presentations to these participants have addressed open source intelligence, not intelligence gathering. The texts of these training presentations can be found on his web site. Applicant was the keynote speaker at a training seminar in Australia. In his answer to the SOR, Applicant also detailed other presentations he made to other

professional organizations while in Australia. Applicant received compensation and travel expenses for these presentations.

Applicant detailed his activities in Canada, explaining that the Canadian Association for Intelligence and Security Studies reimburses him for travel costs and waives their conference fee (subparagraph 1.e.(2)) He also noted his briefing to the Canadian public affairs office on open source intelligence, and a discussion with a representative from the Canadian intelligence service.

As alleged in the SOR at subparagraph 1.e.(3), in 1994, Applicant met with an open source researcher in the Italian ministry, then traveled to England to deliver a presentation on open source intelligence. In 2001, Applicant was paid $5,000.00 for delivering several lectures to the Italian defense intelligence (posted on his web site). Applicant never met the Italian intelligence director.

Applicant conducted a training seminar on open source intelligence (not intelligence gathering) in Germany in 1994 (subparagraph 1.e.(4)), and was paid $2,500.00.

Applicant admitted he conducted training seminars in Belgium (subparagraph 1.e.(5)) on two or three occasions. Applicant provided detailed information about other officials he interfaced with during his trips to Belgium. The military officer referred to in the allegation is actually from Canada; he sponsored Applicant's trip to speak about open source intelligence in 43 countries.

Applicant has traveled to Sweden (subparagraph 1.e.(7)) on three occasions to conduct seminars on open source intelligence. He identified the professor from the university that organized his visits and participation in academic events at the military academy. Applicant provided a week-long, open source training conference to 600 (not 300) attendees. He was paid $20,000.00 and reimbursed for his travel expenses. Subparagraph 1.e.(8) refers to a training conference Applicant sponsored in 1999. While he recalled meeting a Russian military official, he could not remember the other official among the 300 attendees.

Applicant subcontracted open source intelligence work through his defunct company (Company B) as alleged in subparagraph 1.f. of the SOR. Also, he subcontracted open source intelligence work to a permanent U.S. resident who founded the South African open source intelligence unit (subparagraph 1.g.).

Applicant is authorized for access to two facilities (with facility security clearances) companies in his role as individual consultant in the Department of Defense Industrial Security Program (subparagraph 1.i.) Applicant's access as an individual consultant was terminated at three other facilities at the dates set forth in subparagraph 1.j.

In an advertisement on his website (dated June 12, 2003), Applicant offered training courses in an advertisement that indicated "Our DoD Top Secret Collateral clearance is active and can be included in training so as to permit sensitive questions to be asked without difficulty." (subparagraph 1.k.) Applicant has removed the entry from the homepage of his website (AE B, AE C, homepage) Though Applicant indicated in his answer to the SOR that no claim was ever made that his company (Company C) had a facility security clearance, he changed his position after reviewing GE 3, and

stated, "I can see very clearly how this [misrepresentation] is a mistake and could be thought by someone to be in violation." (Tr. 74)

At one time on his resume, Applicant identified himself as Chief Executive Officer of Company C, and that he possessed a Top Secret clearance that was "Codeword" access activated when needed, and that he had a Special Background Investigation (subparagraph 1.l.) Applicant has removed the labels from his resume. (AE C, Resume)

Although Company B and Company C have not possessed a facility security clearance in the Department of Defense Industrial Security Program, and Applicant is not authorized to access to classified information while performing work for either web company, Applicant maintains he has a personal Top Secret clearance (subparagraph 1.m.) to allow members of all the military agencies to ask sensitive questions about open source intelligence.

In the past, Applicant's Company C website indicated his company possessed a "DoD Top Secret, Valid SBI" (subparagraph 1.n.). Applicant deleted the clearance references from his website. (AE C) The second part of subparagraph 1.n. alleges that because Company C has no facility clearance, Applicant is precluded from access to classified information while performing work for Company C. In his answer, Applicant reiterated his position he was authorized to Top Secret access while performing work for Company C under contract to U.S. Agency 1 and U.S. Agency 5. U.S. Agency 1 calls him to their headquarters periodically for classified discussions. Once the task is identified, Applicant testified that he erases the classified information from his memory, and proceeds to resolve the task through open source intelligence avenues to achieve the desired result (Tr. 43-45, 84-86).

Personal Conduct (Guideline E). In October 1999, Applicant completed a security clearance application (SCA) by certifying that:

> My statements on this form, and any attachments to it, are true, complete, and correct to the best of my knowledge and belief and are made in good faith. I understand that a knowing and willful false statement on this for can be punished by a fine or imprisonment or both.

In response to question 14 of the SCA which asked, "Have you ever had any contact with a foreign government, its establishments, (emphasis on consulates), or it representatives, whether inside or outside the U.S., other than official Government business? (Does not include routine visa applications and border crossing contacts)," Applicant answered "no." (subparagraph 2.a.)

In June 2003, Applicant provided a sworn statement explaining open source intelligence and identifying foreign and domestic conferences, seminars, and symposiums conducted since approximately 1993. He also identified certain participants and other individuals who have contributed in some fashion to open source intelligence. Applicant estimated he spent at least 10 hours with the Special Agent in generating the sworn statement (Tr. 51-52).

Applicant certified a second SCA in April 2004. In response to question 14 asking him about contacts with foreign governments, its establishments and representatives, Applicant again answered

"no." (subparagraph 2.b.) In a letter dated January 7, 2005, indicating when and how he intended to prepare and send his answers to the SOR, Applicant interpreted "foreign contacts" to be official foreign contacts or recurring, sustained contacts that he did not have. However, the SCA question does not make the distinction. Applicant viewed the 7,500 contacts (referred to in AE B, letter dated January 10, 2005) as one-time foreign contacts that did not warrant security concern. In his January 24, 2005-answer to the SOR, Applicant considered attendees at his conferences or overseas training sessions to be analogous to visa applications and border crossing contacts. In other correspondence with DOHA before he submitted his answer to the SOR (January 10, 2005), Applicant contended the Special Agent from the Defense Security Service (DSS) who took the sworn statement, agreed with the analogy. There is no documentation of this agreement (between Applicant and the Agent) in GE 3. Applicant did not call the Agent to testify.

At the hearing, Applicant explained he has been dealing with security issues for a long time and has discovered the system cannot handle the information it requests (Tr. 48). Applicant then recounted an example of the system's inability to handle information. After returning from an overseas conference where a Russian intelligence officer spoke to an audience of 300 foreigners, his wife promptly informed her security officer of her trip, and asked him whether he wanted her to report the 300 foreign contacts. He asked her whether she had an affair with any of the those 300 foreigners. When she answered in the negative, he told her to immediately resume her normal duties (Tr. 49).

Applicant claimed he made a mistake in focusing on the last portion of question 14 relating to visa applications and contacts at border crossings (Tr. 50). Applicant reiterated that his foreign contacts were isolated and not sustained. Then, he stated he had a list of 10 sustained contacts that was received in evidence (Tr. 61; AE B). Considering the evidence as a whole, Applicant's explanations for answering "no" twice to question 14 of the SCA forms was not a mistake but an intentional omission of information about his foreign contacts. Omitting the information from his SCA in 1999 could be construed as a mistake. But, omitting the same information a second time from his SCA in April 2004, after spending about 10 hours discussing the subject matter in June 2003, seriously impeaches the credibility of Applicant's explanations. I find Applicant intentionally omitted information concerning his foreign contacts from the two SCA forms.

Character evidence. Applicant enjoys an excellent reputation among those that he has worked. A U.S. congressman considers Applicant the leading expert of open source intelligence, and has contributed the Foreword to two of Applicant's books. In addition, Applicant has authored over 20 articles, presentations, and other written products on the subject of open source intelligence since 1991 (AE C). In January 2006, Applicant conducted a briefing on the coordination of open source intelligence into different communication mediums and information engines.

Applicant is devoted to expanding open source intelligence in all the military agencies as well as other agencies because it is a proven, cost effective method of resolving intelligence requirements. (Tr. 38-40; AE D).

POLICIES

Enclosure 2 of the Directive sets forth guidelines containing disqualifying conditions (DC) and mitigating conditions (MC) that should be given binding consideration in making security clearance determinations. These conditions must be considered in every case along with the general factors of the whole person concept. However, the conditions are not automatically determinative of the decision in any case nor can they supersede the Administrative Judge's reliance on his own common sense.

Burden of Proof

Initially, the government must establish, by substantial evidence, that conditions exist in the personal or professional history of the applicant which disqualifies, or may disqualify, the applicant from being eligible for access to classified information. *See Department of the Navy v. Egan*, 484 U.S. 518, 531 (1988) "[T]he Directive presumes there is a nexus or rational connection between proven conduct under any of the Criteria listed therein and an applicant's security suitability." ISCR Case No. 95-0611 at 2 (App. Bd. May 2, 1996) (quoting DISCR Case No. 92-1106 (App. Bd. Oct. 7, 1993)).

Once the government establishes a disqualifying condition by substantial evidence, the burden shifts to the applicant to rebut, explain, extenuate, or mitigate the facts. "[S]ecurity clearance determinations should err, if they must, on the side of denials." *See Egan*, 481 U.S. at 531; *see* Directive E2.2.2.

Outside Activities (Guideline L)

Involvement in certain types of outside employment activities may pose a conflict with an individual's security responsibilities and could create a risk of unauthorized disclosure of the classified information.

Personal Conduct (Guideline E)

The security concern is that conduct involving questionable judgment or dishonesty could indicate the individual may not properly safeguard classified information.

Criminal Conduct (Guideline J)

A history of pattern of criminal conduct creates doubt about a person's judgment and trustworthiness.

CONCLUSIONS

Outside Activities (OA). A security concern may arise under this guideline when an individual's involvement in outside employment or activities poses a conflict with his security responsibilities to a level that could create an increased risk of unauthorized disclosure of classified information. Conditions that may be disqualifying include any service, whether compensated,

volunteer, or employment with a foreign entity or interest. Applicant's presentations to foreign audiences in foreign countries, and to persons engaging in intelligence or proprietary material invoke the application of OA E2.A12.1.2.1. (*a foreign country*), OA DC E2.A12.1.2.2. (*any foreign national*), OA DC E2.A12.1.2.3. (*a representative of any foreign interest*), and OA DC E2.A12.1.2.4. (*any foreign, domestic, or international organization or person engaged in the analysis, discussion, or publication or material on intelligence, defense, foreign affairs, or protected technology*). Applicant is paid to deliver lectures to foreign and domestic audiences (mostly intelligence officials) while seeking open source intelligence solutions in his consulting assignments for all the military agencies. The government has established a case under the OA guideline.

Having weighed and balanced the evidence from an overall standpoint, I do not find Applicant's primary employment activities pose a conflict with his security responsibilities to his defense contractor or all the military agencies. I find for Applicant under subparagraphs 1.a. through 1.j.(3) based on OA mitigating condition (MC) E2.A12.1.3.1. (*evaluation of the outside employment or activity indicates that it does not pose a conflict with an individual's security responsibilities*). As noted in Findings of Fact, open source intelligence is information (translated in as many languages as possible) received from legal, ethical and appropriate sources. Applicant's business purpose is to teach and engage in open source intelligence (subparagraph 1.a.). Applicant has never had anything to do with "all source endeavors." The unclassified services Applicant's companies have provided to all the military agencies. (subparagraph 1.b.). do not pose a conflict with his security responsibilities. Similarly, Applicant's management of conferences (subparagraphs 1.c. and 1.d.) do not pose a conflict with his security responsibilities either.

Considering the evidence as a whole under subparagraph 1.e., Applicant's training seminars covering open source intelligence in the identified countries, his contacts with and earnings from foreign nationals/organizations do not pose a conflict with his security responsibilities or his defense contractor or his work for the all the military agencies.

Applicant's subcontracting of open source processing work to a foreign owned company (subparagraph 1.f.) and to a resident alien who founded a military open source intelligence unit in South Africa (subparagraph 1.g.). does not interfere with Applicant's security responsibilities.

Applicant traveled to France in 1995 and 1998 (subparagraph 1.h.) to persuade the country officials to become involved in open source in intelligence. In 1998, Applicant spoke at an open source intelligence conference.

Subparagraphs 1.i. and 1.j. are found for Applicant. Applicant's past employment (with authorized access) as an individual consultant at three defense contractors (subparagraph 1.a his current access with two defense contractors as a consultant (with authorized access) does not pose a conflict with his security responsibilities at his current contractor or all the military agencies.

A careful examination of Applicant's answers and his testimony relating to subparagraph 1.k. reflect he has made the remedial changes in order to remove the identified misrepresentation. Applicant has also removed the misrepresentations in subparagraphs 1.l. and 1.n. Accordingly, I find for Applicant under subparagraphs 1.k., 1.l., and 1.n. Based on Applicant's corrective action taken under subparagraphs 1.k., 1.l., and 1.n., I am confident he will continue his corrective action in

bringing himself into complete compliance of Chapter 2, Section 2-213 of the *National Industrial Security Program Operating Manual* (NISPOM), to support his claim of authority for his consulting work for the U.S. Agency 1. My confidence is strengthened by Applicant's devotion to open source intelligence in all the military agencies, his rock solid professional reputation over the last 13 years, and his outstanding security record since 1976.

Personal Conduct (PC). PC DC E2.A5.1.2.2. (*the deliberate omission, concealment of . . . relevant and material facts from any personnel security questionnaire used to determine security clearance eligibility or trustworthiness*) applies to the circumstances of this case. Facts are considered relevant and material when they are capable of influencing an agency decision about an individual's security worthiness. In October 1999, Applicant withheld information from question 14 (foreign contacts) of his SCA. When he was interviewed in June 2003, he was placed on notice his foreign contacts were a security concern. Nonetheless, in April 2004, Applicant answered "no" to the same question. When material information is omitted from an SCA, the omission is excused if the individual forgot or overlooked the information, or misunderstood the question. But with the plethora of foreign contacts Applicant has encountered, it would be difficult to forget or overlook the large number of contacts. Furthermore, Applicant's pre-hearing statements and testimony indicate he did not forget or overlook the information.

Applicant claims he misunderstood the question by interpreting it to apply only to sustained contacts. That interpretation is not credible given the plain meaning of the question that does not differentiate between sustained and incidental contacts. Moreover, with Applicant's age and his military/civilian employment history in intelligence activity, he knew or should have known that foreign contacts were a government concern, especially in his position. While Applicant indicated he made a mistake, his state of mind at the time he filled out the SCAs indicates the deliberate falsification of two SCAs in 1999 and 2004.

The fact that Applicant supplied truthful information during the interview/sworn statement in June 2003 does not excuse the deliberate falsification in 1999 or in 2004. A security clearance applicant must be honest and candid during all phases of the security investigation.

There are four mitigating conditions under the PC guideline that could remove the security concerns triggered by Applicant's deliberate falsifications. PC MC E2.A5.1.3.1. (*the information was unsubstantiated or not pertinent to a determination of judgment and trustworthiness*) does not apply as the omitted information was substantiated and is relevant to a determination of judgment and trustworthiness. PC MC E2.1.3.2. (*the falsification was an isolated incident, was not recent, and the individual has subsequently provided correct information voluntarily*) does not apply because Applicant's deliberate omission occurred in April 2004. PC MC E2.A5.1.3.3. (*the individual made prompt, good-faith efforts to correct the falsification before being confronted with the facts*) does not apply because Applicant's did not correct the omissions of his April 2004 SCA until he prepared and mailed his answers to the SOR in January 2005. PC MC E2.A5.1.3.4. (*omission 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*) must be discussed because of Applicant's claim that the Special Agent misled Applicant about his foreign contacts during the interview in 2003, and should have informed Applicant of the correct meaning of question 14. Applicant's claim regarding the Special Agent fails because he offered no evidence in corroboration.

Furthermore, Applicant did not provide the contact information until he submitted his answer to the SOR. In sum, I find against Applicant under subparagraphs 2.a. and 2.b. of the SOR.

However, I find in Applicant's favor under subparagraphs 2.c. and 2.d. because there is no evidence Applicant deliberately intended to misrepresent his security clearance status and that of his website company (Company C). Applicant merely engaged in a little puffing to enhance his credibility to prospective service providers.

Criminal conduct (CC). Applicant's willful concealment of material information form the DoD violates 18 United States Code (U.S.C.) 1001 and CC DC E2.A10.1.2.1. (*allegations or admission of criminal conduct, regardless of whether the person was formally charged*). The information withheld by Applicant in the SCA forms in 1999 and 2004 had the potential to influence course of the his background investigation in area of legitimate concern to the government. Given the recency of the falsification, CC MC E2.A10.1.3.1. (*the criminal behavior was not recent*) does not apply. Applicant's falsification of two SCAs in a five-year period removes CC MC E2.A10.1.3.2. (*the crime was an isolated incident*) from affirmative consideration. Insufficient time has passed for me to conclude Applicant has satisfied CC MC E2.A10.1.3.6. (*there is clear evidence of successful rehabilitation*), and his ultimate burden of persuasion under subparagraph 3.a. and the CC guideline.

In reaching my decision under the specific guidelines, I have also evaluated this case under the whole person concept. Given Applicant's character evidence and business reputation, Applicant clearly brings himself favorably within the general factors of the whole person model in that I do not find his outside activities pose a conflict with his security responsibilities. However, I cannot excuse or ignore his deliberate falsifications under the whole person model, given his military and civilian, security background, and the fact that between the 1999 SCA and the 2004 SCA, he was placed on notice by a 10 hour security interview/sworn statement in June 2003 that his foreign contacts were a concern to the government.

FORMAL FINDINGS

Formal Findings required by Paragraph 25 of Enclosure 3 are:

Paragraph 1 (Outside Activities, Guideline L): FOR THE APPLICANT.

Subparagraph a. For the Applicant.
Subparagraph b. For the Applicant.
Subparagraph c. For the Applicant.
Subparagraph d. For the Applicant.
Subparagraph e. For the Applicant.
(1) For the Applicant.
(2) For the Applicant.
(3) For the Applicant.
(4) For the Applicant.

(5) For the Applicant.
(6) For the Applicant.
(7) For the Applicant.
(8) For the Applicant.

Subparagraph f. For the Applicant.
Subparagraph g. For the Applicant.
Subparagraph h. For the Applicant.
Subparagraph i. For the Applicant.
(1) For the Applicant.
(2) For the Applicant.
Subparagraph j. For the Applicant.
(1) For the Applicant.
(2) For the Applicant.
(3) For the Applicant.
Subparagraph k. For the Applicant.
Subparagraph l. For the Applicant.
Subparagraph m. For the Applicant.
Subparagraph n. For the Applicant.

Paragraph 2 (Personal conduct, Guideline E): AGAINST THE APPLICANT.

Subparagraph a. Against the Applicant.
Subparagraph b. Against the Applicant.
Subparagraph c. For the Applicant.
Subparagraph d. For the Applicant.

CHECKED WRONG BOX TWICE

Paragraph 3 (Criminal Conduct, Guideline J): AGAINST THE APPLICANT.

Subparagraph a. Against the Applicant.

DECISION

In light of all the circumstances presented by the record in this case, it not clearly consistent with the national interest to grant or continue a security clearance for Applicant.

Paul J. Mason
Administrative Judge