DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 17-00323
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Mary Margaret Foreman, Esq.
For Applicant: *Pro se*

08/31/2018

Decision

HARVEY, Mark, Administrative Judge:

Security concerns under Guidelines K (handling protected information) and E (personal conduct) are not mitigated. Eligibility for access to classified information is denied.

History of the Case

On January 30, 2013, Applicant completed and signed a Questionnaire for National Security Positions (SF 86) or security clearance application (SCA). (Government Exhibit (GE) 1). On September 21, 2017, the Department of Defense (DOD) Consolidated Adjudications Facility (CAF) issued an SOR to Applicant under Executive Order (Exec. Or.) 10865, *Safeguarding Classified Information within Industry*, February 20, 1960; DOD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (Directive), January 2, 1992; and Security Executive Agent Directive 4, establishing in Appendix A new adjudicative guidelines (AGs), effective June 8, 2017.

The SOR detailed reasons why the DOD CAF did not find under the Directive that it is clearly consistent with the interests of national security to grant or continue a security clearance for Applicant, and recommended referral to an administrative judge to determine whether a clearance should be granted, continued, denied, or revoked. Specifically, the SOR set forth security concerns arising under Guidelines K and E. (Hearing Exhibit (HE) 2)

On October 11, 2017, Applicant provided a response to the SOR (HE 3) Department Counsel requested a hearing. (Transcript (Tr.) 13) On March 9, 2018, Department Counsel was ready to proceed. On April 26, 2018, the case was assigned to me. On May 24, 2018, the Defense Office of Hearings and Appeals (DOHA) issued a notice of hearing, setting the hearing for June 12, 2018. (HE 1) Applicant's hearing was held as scheduled.

During the hearing, Department Counsel offered four exhibits; Applicant offered two exhibits; there were no objections; and all proffered exhibits were admitted into evidence. (Tr. 21-24; GE 1-4; AE A-B) On June 21, 2018, DOHA received a copy of the hearing transcript.

Findings of Fact[1]

Applicant's SOR response admitted in part the facts alleged in SOR ¶ 2.b. (HE 3) He also provided mitigating information. Applicant's admissions are accepted as findings of fact. Additional findings of fact follow.

Applicant is a 34-year-old senior engineer. (Tr. 5, 77; GE 1) In 2001, he graduated from high school. (Tr. 6; GE 1) In 2006, he received a bachelor of science degree in information technology management. (Tr. 6) In February 2010, he married. (Tr. 7) He adopted his spouse's child, who was born in 2006. (GE 1) He served in the Army from 2001 to 2008. (Tr. 7) He was deployed to Kuwait in 2003, and Iraq in 2004 and 2006. (Tr. 7-8) His military occupational specialty involved the collection of military intelligence. (Tr. 8) He left active duty as a sergeant (E-5). (Tr. 8) After he left active duty, he deployed to Iraq for about one year working for two different government contractors. (Tr. 30-32)

Collection of Information about Weapons, Explosives, and Body Armor

SOR ¶¶ 2.b(i) through 2.b(vi) allege Applicant conducted Internet research and downloaded videos, pictures, and information on pornography, weapons, body armor, explosives, silencers, conversion of weapons to automatic, and other weapons' modifications. Applicant was going to Iraq, and he said he wanted information that might enhance his safety in a combat zone. (Tr. 26, 49; SOR response) Applicant was on a counter-improvised explosive device (IED) team in Iraq. (Tr. 48) He was not authorized to have a weapon in Iraq as a government contractor. (Tr. 50-51) Applicant contended his research was constitutionally-protected conduct. (Tr. 26-27, 51-55) Applicant objected to investigative questions about his religion. (Tr. 27)[2]

[1] Some details were excluded to protect Applicant's right to privacy. Specific information is available in the cited exhibits.

[2] In accordance with "well established DoD policy [Applicant and his family's] religious affiliation play[ed] no part" in this decision. ISCR Case No. 08-06795 at 6 n. 3 (App. Bd. May 25, 2012).

Removal of Classified Information from a Sensitive Compartmented Information Facility (SCIF)

SOR ¶ 1.a alleges under the handling protected information guideline that in February 2010, Applicant removed a hard drive from a SCIF, downloaded material on his computer from the hard drive, and then returned the hard drive to the SCIF without authorization. SOR ¶ 2.a cross-alleges this conduct under the personal conduct guideline. Applicant used personal hard drives for his contractor duties because it had more storage capacity than the government hard drives. (Tr. 39-40) He also received hard drives from the government containing unclassified information at his home. (Tr. 67) After the security officer at the SCIF scanned his hard drive to ensure there was no virus on it, he was permitted to use it at work. (Tr. 40) He suggested that someone used his hard drive to transfer work data. (Tr. 41) He said he had "unclassified" stickers on his hard drives. (Tr. 41) His team knew which hard drives were Applicant's personal hard drives. (Tr. 42)

SOR ¶¶ 1.b and 2.a allege that in March 2010, a forensic analysis of three unclassified hard drives and two portable unclassified external drives from Applicant's workstation discovered over one million classified documents. A 2010 counter-intelligence investigation indicated a forensic analysis of the media listed in SOR ¶¶ 1.b and 2.a revealed four Top Secret documents created in 2007, and "over a million classified documents" at the Secret level. (GE 3 at 2)

Applicant loaned a hard drive to another employee; that employee discovered a document classified as Secret on it; and he reported this discovery to security. (Tr. 42-44; SOR response) Applicant's employer told him to bring in his home computer and hard drives, and Applicant complied with that direction. (Tr. 43) He said the investigation was closed because there was no evidence that he copied the classified document. (Tr. 44)

Applicant provided a scenario to explain the classified documents on his hard drives and external drives at his residence. He said one of his hard drives had a "Secret" sticker on it. (Tr. 68) The drive was in his office or cubicle area, which had open storage. (Tr. 68-69) Someone may have taken one of his unclassified drives and mixed it in with their property, and then placed the classified information on the drive without putting a classified sticker on it. (Tr. 69) They must have returned the drive with classified information to him, and then Applicant must have taken it home. (Tr. 70) As to the classified information in his possession, he said, "I had no idea of how it got there or why it was there." (Tr. 70)

Applicant suggested that the government reuses hard drives; one of the hard drives the government provided had the classified documents on it at one point; they were not properly deleted; and the government recovered them from Applicant's media. (Tr. 81-82) The classified documents on his media could also have resulted from a dump of a large number of files from Wikileaks or similar public website. (Tr. 82-83; SOR response) Just clicking one Internet link could result in the dump of numerous files on to a computer. (Tr. 82) He blamed his security office for having lax security practices and failure to document transit of computer drives entering and exiting the SCIF. (SOR response)

Transfer of Funds to Citizens and Residents of Foreign Countries

SOR ¶ 2.b(vii) alleges Applicant sent $40,000 to recipients outside the United States via wire transfer; he sent $26,000 to a Columbian national; he sent $7,000 to a foreign account; and he sent funds to bullion and precious metal deposit companies. The bank statements showing the foreign fund transfers were discovered in 2010 when Applicant's computer, hard drives, and external drives were searched for the security investigation involving classified information. (Tr. 80; GE 3 at 3)

While Applicant was deployed to Iraq in the 2008 to 2009 period, he sent $26,000 to his girlfriend (G) who was living in Panama. (Tr. 60-61; SOR response) Shortly thereafter, he suspected he was being exploited in a "romance scam," and he ended his relationship with G. (Tr. 61; SOR response)

Around 2009, Applicant provided $7,000 to a woman in Columbia (S) to enable her to return to Columbia because her passport was stolen. (Tr. 62; SOR response) S was his fiancé. (SOR response) He only knew her about two months. (Tr. 62-63) In 2009, S completed a Foreign Born Spouse Statement of Personal History, and Applicant provided this document to security. (AE B)

Applicant sent $40,000 to his spouse (not S) and her parents to enable them to make home repairs on their home in Nicaragua. (Tr. 57-58; SOR response) In 2012, his spouse returned to Nicaragua while Applicant was deployed to Iraq. (Tr. 59) His spouse now resides in the United States. (Tr. 58) Applicant admitted providing the funds to a Columbian national. (Tr. 56) In 2009, a Foreign Born Spouse Statement of Personal History was completed for his future spouse; however, the form is not signed. (AE A) A note on page 1 indicates it was submitted in 2009 to his security officer. (AE A)

False Statement Denying Payments to Foreign Nationals

SOR ¶ 2.c alleges Applicant falsely denied that he provided financial support to any foreign national on his January 30, 2013 SCA. Applicant disclosed his relationships with his future spouse and S to his security officer; however, his disclosures did not contain information about him providing funds to them. (AE A; AE B) Applicant's January 30, 2013 SCA asks in Section 20A, "Have you **EVER** provided financial support for any foreign national?" (GE 1) (emphasis in original) He answered, no, and he did not disclose on his 2013 SCA that he provided funds to his spouse, his spouse's parents, G, and S. (Tr. 64; GE 1) He understood the question, and he was aware of the money he sent to foreign nationals. (Tr. 70) He explained that his supervisors forced him to hurry to complete his SCA. (Tr. 65, 71) He said he carelessly overlooked the question. (Tr. 65) It was an oversight and "not an intentional attempt to mislead." (Tr. 65)

On his 2013 SCA, Applicant disclosed: his marriage to his spouse; his in-laws' residence in Nicaragua; and spouse's non-citizen status. (GE 1) His 48-page SCA is detailed, and includes information such as a discussion of his security violation in May 2011; allegations against a supervisor of fraud; and complaints about a hostile work environment. (GE 1)

In Applicant's April 24, 2014 Office of Personnel Management (OPM) personal subject interview (PSI), Applicant disclosed in the last four months of 2012, Applicant said he or his spouse transferred $10,000 to $15,000 to his in-laws in Nicaragua.[3] Applicant said he did not disclose the information about his funds transfers "because he was thinking of his in-laws as U.S. persons." (GE 2 at 4) He explained that his mother-in-law had a social security number, had a U.S. visa, and came to the United States three times a year to visit. The investigator confronted Applicant with the funds transfers in 2008 and 2009 as alleged in in SOR ¶ 2.b(vii) and Applicant admitted the transfers. He said he denied the fund transfers on his SCA because he misunderstood the question, and he was in a hurry to complete his SCA. (GE 2 at 6) He was also embarrassed about the fund transfers.

Policies

The U.S. Supreme Court has recognized the substantial discretion of the Executive Branch in regulating access to information pertaining to national security emphasizing, "no one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988). As Commander in Chief, the President has the authority to control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to have access to such information." *Id*. at 527. The President has authorized the Secretary of Defense or his designee to grant applicant's eligibility for access to classified information "only upon a finding that it is clearly consistent with the national interest to do so." Exec. Or. 10865, *Safeguarding Classified Information within Industry* § 2 (Feb. 20, 1960), as amended.

Eligibility for a security clearance is predicated upon the applicant meeting the criteria contained in the adjudicative guidelines. These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, these guidelines are applied in conjunction with an evaluation of the whole person. An administrative judge's overarching adjudicative goal is a fair, impartial, and commonsense decision. An administrative judge must consider all available, reliable information about the person, past and present, favorable and unfavorable.

The Government reposes a high degree of trust and confidence in persons with access to classified information. This relationship transcends normal duty hours and endures throughout off-duty hours. Decisions include, by necessity, consideration of the possible risk the applicant may deliberately or inadvertently fail to safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation about potential, rather than actual, risk of compromise of classified information. Clearance decisions must be "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." *See* Exec. Or. 10865 § 7. Thus, nothing in this decision should be construed to suggest that it is based, in whole or in part, on any express or implied determination about applicant's allegiance, loyalty, or patriotism. It is merely an indication the applicant has not met the strict guidelines the President, Secretary of Defense, and DNI have established for issuing a clearance.

[3] All of the information in this paragraph is from Applicant's April 24, 2014 Office of Personnel Management (OPM) personal subject interview (PSI). (GE 2 at 4-6).

Initially, the Government must establish, by substantial evidence, conditions in the personal or professional history of the applicant that may disqualify the applicant from being eligible for access to classified information. The Government has the burden of establishing controverted facts alleged in the SOR. *See Egan*, 484 U.S. at 531. "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). The guidelines presume a nexus or rational connection between proven conduct under any of the criteria listed therein and an applicant's security suitability. *See* ISCR Case No. 95-0611 at 2 (App. Bd. May 2, 1996).

Once the Government establishes a disqualifying condition by substantial evidence, the burden shifts to the applicant to rebut, explain, extenuate, or mitigate the facts. Directive ¶ E3.1.15. An applicant "has the ultimate burden of demonstrating that it is clearly consistent with the national interest to grant or continue his security clearance." ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002). 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). "[S]ecurity clearance determinations should err, if they must, on the side of denials." *Egan*, 484 U.S. at 531; *see* AG ¶ 2(b).

Analysis

Handling Protected Information

AG ¶ 33 articulates the security concern for drug involvement:

> Deliberate or negligent failure to comply with rules and regulations for handling protected information-which includes classified and other sensitive government information, and proprietary information-raises doubt about an individual's trustworthiness, judgment, reliability, or willingness and ability to safeguard such information, and is a serious security concern.

AG ¶ 34 lists conditions that could raise a security concern and may be disqualifying:

> (a) deliberate or negligent disclosure of protected information to unauthorized persons, including, but not limited to, personal or business contacts, the media, or persons present at seminars, meetings, or conferences;
>
> (b) collecting or storing protected information in any unauthorized location;
>
> (c) loading, drafting, editing, modifying, storing, transmitting, or otherwise handling protected information, including images, on any unauthorized equipment or medium;
>
> (d) inappropriate efforts to obtain or view protected information outside one's need to know;

(e) copying or modifying protected information in an unauthorized manner designed to conceal or remove classification or other document control markings;

(f) viewing or downloading information from a secure system when the information is beyond the individual's need-to-know;

(g) any failure to comply with rules for the protection of classified or sensitive information;

(h) negligence or lax security practices that persist despite counseling by management; and

(i) failure to comply with rules or regulations that results in damage to the national security, regardless of whether it was deliberate or negligent.

SOR ¶ 1.a alleges under the handling protected information guideline that in February 2010, Applicant removed a hard drive from a SCIF, downloaded material on his computer from the hard drive, and then returned the hard drive to the SCIF without authorization. Applicant said he was authorized to bring hard drives into the SCIF and to remove hard drives from the SCIF. No evidence from witnesses, a standard operating procedure, or similar source was presented to contradict his statement about being authorized to handle the hard drives in this manner. SOR ¶ 1.a is found for Applicant.

SOR ¶ 1.b alleges, and the record establishes that in 2010, a counter-intelligence forensic analysis on three hard drives and two portable external drives that Applicant had at his residence discovered over one million classified documents on this media. There was no evidence presented that Applicant was authorized to store classified information at his residence. AG ¶¶ 34(b), 34(c), and 34(g) are established.

AG ¶ 35 lists conditions that could mitigate security concerns:

(a) so much time has elapsed since the behavior, or it has happened so infrequently or under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or good judgment;

(b) the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities;

(c) the security violations were due to improper or inadequate training or unclear instructions; and

(d) the violation was inadvertent, it was promptly reported, there is no evidence of compromise, and it does not suggest a pattern.

The DOHA Appeal Board in ISCR Case No. 10-04641 at 4 (App. Bd. Sept. 24, 2013), concisely explained Applicant's responsibility for proving the applicability of mitigating conditions as follows:

> Once a concern arises regarding an Applicant's security clearance eligibility, there is a strong presumption against the grant or maintenance of a security clearance. *See Dorfmont v. Brown*, 913 F. 2d 1399, 1401 (9th Cir. 1990), *cert. denied*, 499 U.S. 905 (1991). After the Government presents evidence raising security concerns, the burden shifts to the applicant to rebut or mitigate those concerns. *See* Directive ¶ E3.1.15. The standard applicable in security clearance decisions is that articulated in *Egan*, *supra*. "Any doubt concerning personnel being considered for access to classified information will be resolved in favor of the national security." Directive, Enclosure 2 ¶ 2(b).

None of the mitigating conditions apply. In 2010, Applicant had three hard drives and two portable external drives at his residence. Over a million classified documents were found on this media. Applicant did not provide a credible explanation for these documents being on his media at his home. Handling protected information security concerns are not mitigated.

Personal Conduct

AG ¶ 15 articulates the security concern for personal conduct:

> Conduct involving questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations can raise questions about an individual's reliability, trustworthiness, and ability to protect classified or sensitive information. Of special interest is any failure to cooperate or provide truthful and candid answers during national security investigative or adjudicative processes. The following will normally result in an unfavorable national security eligibility determination, security clearance action, or cancellation of further processing for national security eligibility:

AG ¶ 16 lists conditions that could raise a security concern and may be disqualifying in this case including:

> (a) deliberate omission, concealment, or falsification of relevant facts from any personnel security questionnaire, personal history statement, or similar form used to conduct investigations, determine employment qualifications, award benefits or status, determine national security eligibility or trustworthiness, or award fiduciary responsibilities;
>
> (c) credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any other single guideline, but which, when considered as a whole, supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other

characteristics indicating that the individual may not properly safeguard classified or sensitive information;

(d) credible adverse information that is not explicitly covered under any other guideline and may not be sufficient by itself for an adverse determination, but which, when combined with all available information, supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the individual may not properly safeguard classified or sensitive information. This includes, but is not limited to, consideration of:

(1) untrustworthy or unreliable behavior . . . ;

(2) any disruptive, violent, or other inappropriate behavior;

(3) a pattern of dishonesty or rule violations; and

(e) personal conduct, or concealment of information about one's conduct, that creates a vulnerability to exploitation, manipulation, or duress by a foreign intelligence entity or other individual or group. Such conduct includes: (1) engaging in activities which, if known, could affect the person's personal, professional, or community standing.

SOR ¶ 2.a alleges the same conduct that is alleged in the previous section. This conduct is sufficient for an adverse determination without recourse to the personal conduct guideline, and AG ¶¶ 16(c) and 16(d) do not apply. His conduct in SOR ¶ 2.a is known to security officials, and threats of public disclosure would not cause him to compromise classified information. AG ¶ 2.a is mitigated as a duplication.

Applicant conducted Internet research and downloaded videos, pictures, and information on pornography, weapons, body armor, explosives, silencers, conversion of weapons to automatic, and other weapons' modifications. Applicant's research is constitutionally-protected conduct. He has a right under the First Amendment to obtain and possess such information. There is no evidence that he used the information for any illegal purpose. Applicant sent money to people in Central America and Columbia. Funds transfers are not illegal. They may raise foreign influence concerns; however, the transfers are not alleged under Guideline B. AG ¶ 2.b is found for Applicant because the financial transactions, without more information, do not independently raise a security concern under Guideline E.

Applicant falsely denied that he provided financial support to any foreign national on his January 30, 2013 SCA. He did not disclose on his 2013 SCA that he paid a total of over $70,000 to his spouse, his spouse's parents, G, and S. In his OPM PSI, he said he did not understand the question. At his hearing, he said he understood the question. Applicant is intelligent. I specifically find that he understood the question, and he intentionally elected not to disclose accurate information about payments to foreign

nationals. AG ¶ 16(a) is established requiring additional inquiry about the possible applicability of mitigating conditions.

Six personal conduct mitigating conditions under AG ¶ 17 are potentially applicable in this case:

> (a) the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts;
>
> (b) the refusal or failure to cooperate, omission, or concealment was caused or significantly contributed to by advice of legal counsel or of a person with professional responsibilities for advising or instructing the individual specifically concerning security processes. Upon being made aware of the requirement to cooperate or provide the information, the individual cooperated fully and truthfully;
>
> (c) the offense is so minor, or so much time has passed, or the behavior is so infrequent, or it happened under such unique circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment;
>
> (d) the individual has acknowledged the behavior and obtained counseling to change the behavior or taken other positive steps to alleviate the stressors, circumstances, or factors that contributed to untrustworthy, unreliable, or other inappropriate behavior, and such behavior is unlikely to recur;
>
> (e) the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress; and
>
> (f) the information was unsubstantiated or from a source of questionable reliability.

None of the mitigating conditions apply. Applicant falsely denied that he provided financial support to any foreign national on his January 30, 2013 SCA. He did not disclose on this SCA that he paid a total of over $70,000 to his spouse, his spouse's parents, G, and S when they were citizens and residents of foreign countries. I do not believe his claim that the falsification was inadvertent or unintentional. His false statement is recent, serious, and not mitigated.

Whole-Person Concept

Under the whole-person concept, the administrative judge must evaluate an Applicant's eligibility for a security clearance by considering the totality of the Applicant's conduct and all the circumstances. The administrative judge should consider the nine adjudicative process factors listed at AG ¶ 2(d):

> (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 extent to which participation is voluntary; (6) the presence or absence of rehabilitation and other permanent 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.

Under AG ¶ 2(c), "[t]he ultimate determination" of whether to grant a security clearance "must be an overall commonsense judgment based upon careful consideration of the guidelines" and the whole-person concept. My comments under Guidelines K and E are incorporated in my whole-person analysis. Some of the factors in AG ¶ 2(d) were addressed under those guidelines but some warrant additional comment.

Applicant is a 34-year-old senior engineer. In 2006, he received a bachelor of science degree in information technology management. He served in the Army from 2001 to 2008. He completed tours in Kuwait in 2003, and Iraq in 2004 and 2006. He left active duty as a sergeant. After he left active duty, he deployed to Iraq for about one year working for two different government contractors.

The evidence against granting his security clearance is more persuasive. Applicant had three hard drives and two portable external drives at his residence. Over a million classified documents were found on this media. He did not provide a credible explanation for these classified documents being in his possession at his residence.

Applicant falsely denied that he provided financial support to any foreign national on his January 30, 2013 SCA. He did not disclose on his 2013 SCA that he paid a total of over $70,000 to his spouse, his spouse's parents, G, and S when they were citizens and residents of foreign countries. His statements about carelessly overlooking the question; that it was an oversight; and that it was not an intentional attempt to mislead are not credible. His false statement on his 2013 SCA was deliberate, improper, and made with intent to deceive. AG ¶ 15 indicates, "Of special interest is any failure to cooperate or provide truthful and candid answers during national security investigative or adjudicative processes." Applicant's falsifications raise serious security concerns. The protection of national security relies on applicants to self-report conduct that jeopardizes security, even when that disclosure might damage the applicant's career. Applicant cannot be trusted to disclose potentially derogatory information related to security issues. He did not establish his reliability, trustworthiness, and ability to protect classified information.

I have carefully applied the law, as set forth in *Egan,* Exec. Or. 10865, and the AGs, to the facts and circumstances in the context of the whole person. Guidelines K and E security concerns are not mitigated.

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 K:	AGAINST APPLICANT
Subparagraph 1.a:	For Applicant
Subparagraph 1.b:	Against Applicant
Paragraph 2, Guideline E:	AGAINST APPLICANT
Subparagraphs 2.a and 2.b:	For Applicant
Subparagraph 2.c:	Against Applicant

Conclusion

In light of all of the circumstances in this case, it is not clearly consistent with the interests of national security to grant Applicant eligibility for a security clearance. Eligibility for access to classified information is denied.

_____
Mark Harvey
Administrative Judge