DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
----------	)	ISCR Case No. 15-03293
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Caroline Heintzelman, Esquire, Department Counsel
For Applicant: *Pro se*

06/08/2016

Decision

HOWE, Philip S., Administrative Judge:

On November 21, 2012, Applicant submitted his Electronic Questionnaire for Investigations Processing (e-QIP). On June 12, 2015, the Department of Defense Consolidated Adjudications Facility (DODCAF) issued Applicant a Statement of Reasons (SOR) detailing security concerns under Guidelines K (Handling Protected Information) and E (Personal Conduct). The action was taken under Executive Order 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the adjudicative guidelines (AG) effective within the Department of Defense on September 1, 2006.

Applicant acknowledged receipt of the SOR on June 29, 2015. He answered the SOR in writing on July[1] 12, 2015, and requested a hearing before an administrative judge. The Defense Office of Hearings and Appeals (DOHA) received the request shortly after July 14, 2015 when he mailed it to DOHA. Department Counsel was prepared to proceed on October 16, 2015, and I received the case assignment on October 29, 2015.

DOHA issued a Notice of Hearing on November 18, 2015, and I convened the hearing as scheduled on December 8, 2015. The Government offered Exhibits 1 through 4, which were received without objection. Applicant testified on his own behalf, called two additional witnesses, and submitted Exhibits A and B, without objection. He also submitted his opening and closing statements, which I marked as Exhibits C and D.

DOHA received the transcript of the hearing (Tr.) on December 16, 2015. Based upon a review of the pleadings, exhibits, and testimony, eligibility for access to classified information is denied.

Findings of Fact

In his Answer to the SOR Applicant admitted the factual allegations in ¶¶ 1.a, 1.b, 1.c, 1.d and 1.f of the SOR, with explanations. He denied the factual allegations in ¶ 1.e of the SOR. He denied ¶¶ 2.a and 2.b of the SOR. He also provided additional information to support his request for eligibility for a security clearance.

Applicant is 70 years old. He is married and has five adult children. He is employed by a defense contractor as a manager. He has a master's degree and has worked for the same defense contractor for 26 years. Applicant's first security clearance was in May 1963 after he graduated from high school and worked a summer job as an aide at a government facility. He served as an officer in the U.S. military from 1969 to 1989 and had a security clearance. He has held one while working for the defense contractor after his military retirement. Pending this case disposition, his clearance was suspended in January 2015. (Tr. 28-32, 57; Exhibits 1, 3 at page 12)

Applicant failed to comply with security requirements in June 2010 when he failed to properly secure a classified area. He received additional education for alarms, securing facilities, and security monitoring duties (Subparagraph 1.a). He admitted this allegation. His contention about the incident is stated in his Answer. He wrote that he has closed and alarmed this area for more than 25 years. He stated security is in place

[1] His Answer and transmittal documents state the date on each as June 12, 2015. However, that is the date of the SOR, so it would be impossible for a six page Answer to be written and sent on the same day as the SOR; Applicant must have meant "July 12, 2015" as the date of his Answer. I use that logical date in this Decision.

all the time and the location of the room is deep inside the company's building with constant security. But Applicant entered the room at 1413 hours and deactivated the alarm. He performed the work he intended and departed the room at 1630 hours, anticipating returning to the room so he did not reset the alarm. Applicant admitted "completely forgetting" to reset the alarm. The security infraction was reported to the company and an investigation was initiated. An administrative inquiry followed, a copy of which is included as Exhibit 4. It will be purged from the company files in June 2020. (Tr. 33-36; Exhibit 4 at page 1)

Applicant failed to comply with security requirements in March 2011 when he failed to properly secure a program area by failing to activate an intrusion detection system (Subparagraph 1.b). He admitted this incident, which involved his forgetting to set the alarm for a program area for a night. He claims that anyone entering this area needs a badge and a PIN number. It is his daily work area and he has been working there for 25 years. He also states any classified material in the room is locked in security containers nightly. Applicant wrote that investigations showed no classified information was compromised or released. He denies any written warning, suspension, reprimand, or disciplinary actions were taken. Applicant also states that since 2011 his company has used a security guard check and an indicator light system to make certain the areas are locked as required. An administrative inquiry was conducted on this incident. The security manager commented at the end of the report was that he spoke to Applicant about the incident and its seriousness. (Tr. 36-41; Exhibit 4 at pages 6 and 7; Answer)

Applicant admitted he committed a security infraction in August 2012, which resulted in the possible compromise of classified information, when he sent a classified email containing improper markings that resulted in a data spill (Subparagraph 1.c). He received a verbal warning for this infraction. Applicant sent an email on a "closed, secure, classified email system, not on a public or unclassified company email system," according to his Answer on Page 2. He claims it was reported to the company and government for investigation and that no classified information was compromised or released. Applicant testified it was late on a work day and he was tired when the incident occurred. He did not report it as he attempted to recall the message and wipe it from the system, calling it a mistake. (Tr. 41-46, 59; Exhibit 4 at pages 8, 14; Answer)

In March 2013 Applicant admitted he committed a security violation when he transmitted classified information on a secure network not approved for that information (Subparagraph 1.d). He sent an email to a customer who deemed the transmission was not made in the proper transmittal system. Applicant claimed the recipient was a "new guy" to the system, but did not provide any evidence to support his claims. Applicant told the government investigator he had sent the information four times using the same system and no one complained. He denied he transmitted classified information to unauthorized persons. When notified of the data spill, he failed to report the security

violation. He received a Corrective Action Memorandum (CAM) from his employer, which noted that there was a prior incident within the previous 12 months, being the August 2012 incident. (Tr. 46-54; Exhibits 2, 3, 4 at page 10; Answer)

In April 2013 Applicant admitted he committed a security violation when he submitted classified information over multiple secured networks not approved for such information (Subparagraph 1.e). There was a data spill. He received a CAM. Applicant denies prior knowledge of this incident being included in the CAM until he read about it in the SOR. This violation was discovered by government agents. The administrative inquiry cites the August 2012 and April 2013 incidents, naming the first as a "security infraction" and the second as a "security violation." Applicant states the incidents set forth in Subparagraphs 1.d and 1.e were combined without specifics in this one memorandum. He claims no classified information was compromised although a "spill" occurred on a closed network. He lost his access to the system from mid-April to the beginning of June 2013. (Tr. 54-55, 88; Exhibits 2, 4 at page 12; Answer)

Applicant committed a security violation when he transmitted classified information in September 2014 on a network not approved for such information (Subparagraph 1.f). Applicant admits this incident, but claims it was a "Security Infraction" instead of a "Security Violation." He states the network is secure at a level consistent with the information. (Tr. 40, 55; Exhibit 3 at page 10; Answer)

All of these incidents involving Applicant were violations of the requirements of the National Industrial Security Program Operating Manual (NISPOM) provisions for protection of classified information. Applicant attempts in his written opening statement to draw a distinction between "infractions" and "violations." He contends no classified information was released to the public. (Exhibit 4)

Under the personal conduct guidelines, Applicant is alleged to have falsified material facts on his e-QIP on November 21, 2012, in Section 13A by failing to disclose the verbal reprimand given him in August 2012 as alleged in SOR Subparagraph 1.c. He denies deliberately falsifying his e-QIP. He argues that in the previous seven years he had not received a written warning or been officially reprimanded, suspended, or disciplined for misconduct. None of the incidents sited in Paragraph 1 met this requirement, he contends. He states he misunderstood the questions because he was never official reprimanded or warned. He states the verbal reprimand was "reeducation" and was not punitive. (Tr. 60; Exhibit 1; Answer)

In an interview on August 9, 2013, it is alleged Applicant deliberately provided false information to a U.S. Defense Department investigator regarding security infractions or violations in the previous seven years, He disclosed the March 2013 incident, but not the other four incidents alleged in the SOR subparagraphs 1.a to 1.c, and 1. e. Applicant denies this allegation of falsification. He claims he disclosed the

incident in Subparagraph 1.d, but was unaware of the Subparagraph 1.e. incident because it was combined in the same CAM, as he explained in response to the allegation in Subparagraph 1.e. The CAM specifically refers to both the March 5, 2013 and April 1, 2013 incidents. It also states, "Applicant received a verbal warning for a security violation that occurred in August 2012." This CAM is dated April 15, 2013 and warns Applicant that further incidents could involve a review of additional "corrective action, up to and including discharge from the Company." It is dated before Applicant's interview with the government investigator in August 2013. (Tr. 53, 54; Exhibit 4)

Applicant was interviewed by the government investigator between August 9 and September 2, 2013. Applicant disputes the accuracy of the investigator's summary as it pertains to his reports of his security violations. He wrote a seven page response to interrogatories sent him by DOHA about the security violations answers. He claims he thought the investigator was asking about incident since the November 21, 2012 completion of the e-QIP, and not the seven previous years. He also contends previous emails to the same customers were sent over the same email system with the same program identifiers (PID). He blames a new member of the group receiving the emails, who was not familiar with the precedents and complained about alleged improper PID and not the content of the classified email. The company investigated and Applicant signed a CAM. (Tr. 58, 59; Exhibit 3)

Applicant's interrogatories' response continues to state that he thought Section 13A referred only to security violations in the past seven years. The question in Section 13A asks if Applicant had "received a written warning, been officially reprimanded, suspended, or disciplined for misconduct in the workplace, such as a security violation." The term "security violation" is used as one example of misconduct. Applicant incorrectly interpreted it to be the only type of workplace misconduct he needed to disclose, thereby not making full disclosure as required, but engaging in his own interpretation of Section 13A's scope. (Tr. 60-63, 66; Exhibits 3, A)

Applicant referred to his Exhibit A at pages 12 and 13 to explain the difference between a "security violation" and a "security infraction." He claims that the essential difference is that with a violation a "loss, compromise or suspected compromise of classified information" is involved. An infraction is "any other incident that is not in the best interest of security that does not involve the loss or compromise or suspected compromise of classified information." They are to be documented so they can be reviewed by higher authority later. Applicant contends his security incidents did not compromise classified information. Applicant testified he did not receive a written warning, official reprimand, suspension, or discipline before he completed the e-QIIP in November 2012. He and his first witness, his manager, stated only a company director can administer discipline. (Tr. 64- 67, 91-93; Exhibit A)

Applicant then discloses that the 2010 and 2011 security incidents were a failure to set an alarm for an office where he worked, claiming that the office was protected by overlapping security systems even if he did not set the alarm. He admits he was verbally advised how to prevent future errors, "but no written warning, suspension, reprimand, or disciplinary actions were taken." Again, Applicant applies his own interpretation to actions and events instead of making full disclosure and allowing the government to sort out the facts. (Exhibit 3 at pages 9 and 10)

Applicant explains the August 16, 2012 incident as his "inadvertently manually" typing a PID into an unauthorized but secure network. He reported it and his actions were judged to be an "administrative infraction," though he does not state who made the judgment. He claims no information was released to persons outside the company. (Exhibit 3 at page 10)

Applicant's interrogatory response goes on to address his latest incident on September 26, 2014, regarding a power point file alteration he was directed to perform. The error was corrected, he states. Again, Applicant insists he never received a written warning and not been officially reprimanded, suspended, or disciplined for these incidents or for any misconduct in the workplace in the past seven years. (Exhibit 3 at page 10)

Applicant had two character witnesses testify. One was his immediate superior for the past 24 years. He was aware of Applicant's infractions and violations. He retired from the employing company in March 2014. He testified that all of Applicant's incidents were "infractions," except the March 2013 incident, which was a violation (Subparagraph 1.d). This witness gave Applicant a verbal warning for the August 2012 incident. The witness stated the March 2011 incident did not result in a written reprimand or warning. He also stated the employing defense contractor held Applicant in high regard. (Tr. 76-88, 113)

The other witness is a director of the company. He has known Applicant for about 20 years. This witness also retired from the U.S. military. He stated Applicant needs a security clearance to perform his job. (Tr. 115-127)

Policies

When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the adjudicative guidelines (AG). In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially disqualifying conditions and mitigating conditions, which are useful in evaluating an applicant's eligibility for access to classified information.

These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, these guidelines are applied in conjunction with the factors listed in the adjudicative process (AG ¶ 2(a)). The administrative judge's overarching adjudicative goal is a fair, impartial, and commonsense decision. According to AG ¶ 2(c), the entire process is a conscientious scrutiny of a number of variables known as the "whole-person concept." The administrative judge must consider all available, reliable information about the person, past and present, favorable and unfavorable, in making a decision.

The protection of the national security is the paramount consideration. AG ¶ 2(b) requires that "[a]ny doubt concerning personnel being considered for access to classified information will be resolved in favor 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.

Under Directive ¶ E3.1.14, the Government must present evidence to establish controverted facts alleged in the SOR. Under Directive ¶ E3.1.15, an "applicant is responsible for presenting witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by the applicant or proven by Department Counsel, and has the ultimate burden of persuasion as to obtaining a favorable clearance decision."

A person who seeks access to classified information enters into a fiduciary relationship with the Government predicated upon trust and confidence. This relationship transcends normal duty hours and endures throughout off-duty hours. The Government reposes a high degree of trust and confidence in individuals to whom it grants access to classified information. Decisions include, by necessity, consideration of the possible risk the 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.

Section 7 of Executive Order 10865 provides that 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." *See also* EO 12968, Section 3.1(b) (listing multiple prerequisites for access to classified or sensitive information).

Analysis

Guideline K, Handling Protected Information

AG ¶ 33 expresses the security concern pertaining to handling protected information, "Deliberate or negligent failure to comply with rules and regulations for

protecting classified or other sensitive 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 describes nine conditions that could raise a security concern and may be disqualifying. Four conditions may apply:

> (a) deliberate or negligent disclosure of classified or other protected information to unauthorized persons, including but not limited to personal or business contacts, to the media, or to persons present at seminars, meetings, or conferences;
>
> (c) loading, drafting, editing, modifying, storing, transmitting, or otherwise handling classified reports, data, or other information on any unapproved equipment including but not limited to any typewriter, word processor, or computer hardware, software, drive, system, gameboard, handheld, "palm" or pocket device or other adjunct equipment;
>
> (g) any failure to comply with rules for the protection of classified or other sensitive information; and
>
> (h) negligence or lax security habits that persist despite counseling by management.

Applicant committed six incidents of failing to comply with rules and regulations of the U.S. government and his employing defense contractor regarding the securing and proper transmitting of classified information. These incidents occurred in June 2010, March 2011, August 2012, March 2013, and April 2013. These incidents involved not setting an alarm at the company office in 2010 and 2011. Then he transmitted classified information improperly in 2012, twice in 2013, and 2014. Applicant did not report the March 2013 incident to his superiors. He received a verbal warning in connection with the August 2012 incident. Then he received a CAM for the two 2013 incidents.

Applicant committed these incidents negligently, particularly the transmittal incidents. He blamed tiredness and forgetfulness for the failures to properly set alarms. AG¶ 34 (a) and (c) are established.

Applicant could not follow the rules and regulations pertaining to protecting and transmitting classified information. He did not comply with alarm setting requirements. AG ¶ 34 (g) and (h) apply because the six incidents show Applicant would not comply with security requirements, even after receiving verbal warnings and the CAM for two incidents. These incidents, regardless of whether they are "violations" or "infractions,"

demonstrate a pattern of non-compliance by an experienced person who has worked a long time for a defense contractor.

AG ¶ 35 provides three conditions that could mitigate security concerns. I conclude none of them apply:

> (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; and
>
> (c) the security violations were due to improper or inadequate training.

Applicant's security incidents occurred six times over a four year period. Two occurred within a month of each other in 2013. These are not infrequent or occurring under unusual circumstances. They occurred in his normal work environment. His last violation was in September 2014 and his security clearance was suspended in January 2015, so no further incidents have occurred. The one year elapsing since his clearance suspension, or even counting from September 2014, is not much time. AG ¶ 35 (a) is not established.

Applicant had six incidents in four years. He obviously did not respond favorably to counseling or remedial training. He argued definitions and types of disciplinary actions within his employing company rather than addressing the security issues. AG ¶ 35 (b) is not established.

Applicant had a long history of working for this company. He also had military experience as an officer. He has had security clearances since sometime in the 1960s. He should have known how to handle these situations, but failed to do so. His training has been over his adult life .The incidents were not due to any improper or inadequate training. AG ¶ 35 (c) is not established.

Guideline E, Personal Conduct

AG ¶ 15 expresses the security concern pertaining to 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 information. Of special interest is any failure to provide truthful and candid answers during the security clearance process or any other failure to cooperate with the security clearance process.

The following will normally result in an unfavorable clearance action or administrative termination of further processing for clearance eligibility:

(b) refusal to provide full, frank and truthful answers to lawful questions of investigators, security officials, or other official representatives in connection with a personnel security or trustworthiness determination.

AG ¶ 16 describes seven conditions that could raise a security concern and may be disqualifying. Four conditions may apply:

(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 security clearance eligibility or trustworthiness, or award fiduciary responsibilities;

(b) deliberately providing false or misleading information concerning relevant facts to an employer, investigator, security official, competent medical authority, or other official government representative;

(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 person may not properly safeguard protected information. This includes but is not limited to consideration of:

(1) untrustworthy or unreliable behavior to include breach of client confidentiality, release of proprietary information, unauthorized release of sensitive corporate or other government protected information: and

(3) a pattern of dishonesty or rule violations.

(e) personal conduct, or concealment of information about one's conduct, that creates a vulnerability to exploitation, manipulation, or duress, such as (1) engaging in activities which, if known, may affect the person's personal, professional, or community standing, or (2) while in another

country, engaging in any activity that is illegal in that country or that is legal in that country but illegal in the United States and may serve as a basis for exploitation or pressure by the foreign security or intelligence service or other group.

Applicant deliberately concealed security violations incidents in response to Section 13A of the e-QIP he completed in 2012. The full disclosure requirements in answering the e-QIP questions were set forth in the instructions, and Applicant confirmed the truthfulness of his answers when he signed the e-QIP. However, he did not report any of the three incidents that occurred before he signed the e-QIP. When questioned by the government investigator in August 2013 he disclosed only one security violation that occurred in March 2013. Applicant tried to justify his non-disclosure on the e-QIP and to the investigator by using his personal definitions of what needed to be disclosed. He did not make full disclosure of the April 2013 incident, nor is there a record of the 2010, 2011, and August 2012 incidents. Therefore, AG ¶ 16 (a) and (b) are established.

Applicant engaged in behavior demonstrating he could not comply with his employer's security requirements through his unauthorized release of protected information over several computer systems between 2012 and 2014. AG ¶ 16 (d) is established because of the pattern of rule violations.

Applicant's personal conduct in concealing the full array of his security violations creates a vulnerability to exploitation, manipulation, and duress because the concealment and sophistry in which he engaged about his activities, if known, would affect his personal, professional, or community standing. AG ¶ 16 (e) is established.

AG ¶ 17 provides seven conditions that could mitigate security concerns. None of them apply:

(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 improper or inadequate advice of authorized personnel or legal counsel advising or instructing the individual specifically concerning the security clearance process. 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 caused 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;

(f) the information was unsubstantiated or from a source of questionable reliability; and,

(g) association with persons involved in criminal activity has ceased or occurs under circumstances that do not cast doubt upon the individual's reliability, trustworthiness, judgment, or willingness to comply with rules and regulations.

Applicant continued to maintain, at the hearing, his nuancing and characterizations of his security incidents, intending to persuade that they did not meet the full disclosure requirements of the e-QIP. However, his arguments were not credible in view of the pattern of incidents, particularly as they increased over the years in 2013 and 2014. Applicant should have made full disclosure, explained any characterization in the "Additional Comments" portion of the e-QIP, or discussed them with the investigator at the interview after he wrote his full disclosure in answering Section 13A of the e-QIP. Applicant is not authorized to decide what parts of what information he would disclose when the lead paragraph of the e-QIP put him on notice that it required him to "complete and truthfully" answer all questions. Therefore, no mitigating condition applies.

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 an applicant's conduct and all the circumstances. The administrative judge should consider the nine adjudicative process factors listed at AG ¶ 2(a):

(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.

AG ¶ 2(c) requires each case must be judged on its own merits. Under AG ¶ 2(c), the ultimate determination of whether to grant eligibility for a security clearance must be an overall commonsense judgment based upon careful consideration of the guidelines and the whole person concept.

I considered the potentially disqualifying and mitigating conditions in light of all the facts and circumstances surrounding this case. Applicant is an experienced employee of a defense contractor who has had security clearances for nearly 40 years. He knew the security incidents should have been revealed on the e-QIP and then discussed with an investigator. Instead, he made his own decisions about what needed to be disclosed to the U.S. government, which were not complete and truthful, as required. He would have had ample opportunity to discuss the nuances of his security violations if he had disclosed them all and added additional comments at the end of the e-QIP. Furthermore, he did not make full disclosure to the government investigator so that his security incidents could be discussed and evaluated. While testifying, he took little responsibility for his behaviors or demonstrated remorse.

Overall, the record evidence leaves me with serious questions or doubts as to Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude Applicant did not mitigate the security concerns arising from his Handling Protected Information and Personal Conduct security concerns.

Formal Findings

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

Paragraph 1, Guideline K:	AGAINST APPLICANT
Subparagraph 1.a:	Against Applicant
Subparagraph 1.b:	Against Applicant
Subparagraph 1.c:	Against 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

Conclusion

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

PHILIP S. HOWE
Administrative Judge