DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	
----------	)	ISCR Case No. 15-01014
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Andrew Henderson, Esq., Department Counsel
For Applicant: Todd M. Hinnen, Esq.

10/05/2016

Decision

WESLEY, Roger C., Administrative Judge:

Based upon a review of the pleadings, exhibits, and testimony, I conclude that Applicant did not mitigate personal conduct concerns. Eligibility for access to classified information is denied.

Statement of Case

On September 30, 2015, the Department of Defense (DoD) Consolidated Adjudications Facility (CAF) issued a Statement of Reasons (SOR) detailing reasons why DoD adjudicators could not make the affirmative determination of eligibility for a security clearance, and recommended referral to an administrative judge to determine whether a security clearance should be granted, continued, denied, or revoked. The action was taken under Executive Order 10865, *Safeguarding Classified Information Within Industry* (February 20, 1960), as amended; DoD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the Adjudicative Guidelines (AGs) implemented by DoD on September 1, 2006.

Applicant responded to the SOR on November 7, 2015, and requested a hearing. The case was assigned to me on April 7, 2016, and was scheduled for hearing on April 27, 2016. At hearing, the Government's case consisted of six exhibits (GEs 1-5). Applicant relied on one witness (himself) and three exhibits (AEs A-C). The transcript (Tr.) was received on May 10, 2016.

Procedural Issues

Applicant interposed objections to the admission of GEs 2-5 on grounds they represented pleadings and responses in a lawsuit that was settled without any of the parties admitting wrongdoing. The Government cited to a number of allegations in the global civil complaint filed in federal court in August 2010 that Applicant admitted. Considering all of the facts and arguments of the parties, GEs 2-5 were admitted conditionally for the limited purpose of considering fact admissions to allegations in the complaint. (Tr. 25-27) Applicant's objection to the admission of GE 6 on grounds of hearsay of a trade publication was sustained.

Summary of Pleadings

Under Guideline E, Applicant allegedly was a named defendant in a civil complaint filed against himself, his father, his father's company (Company A), and several others in August 2010 by a corporate competitor (Company B) alleging a multi-year scheme of fraud and industrial espionage. Allegedly, by operating as a representative of a shell company (Company C), Applicant obtained Company B software for other Company A employees who used it to create programs designed to enable Company B customers to export data of Company B software to make Company A more competitive. Allegedly, the parties reached a settlement in February 2011 that included a condition that Company A pay Company B a lump sum of $11 million in damages and remove all Company B import/export features of Company A software.

Under Guideline E, Applicant allegedly falsified material facts in his electronic questionnaires for investigations processing (e-QIP) of April 1, 2014 when responding to question 28 by answering "no" to the question of whether he was a party to any public record civil complaint not listed elsewhere in the e-QIP.

In his response to the allegations of subparagraph 1.a of the SOR, Applicant admitted some of the allegations. More specifically, he admitted Company B's filing a complaint in federal court in August 2010 and reaching a settlement with the named defendants in February 2011 that consisted of a payment by Company A to Company B in the amount of $11 million and the removal and return by Company A of all Company B property. Applicant denied the remaining allegations covered by subparagraph 1.a.

Responding to subparagraph 1.b of Guideline E, Applicant admitted his failure to disclose the civil complaint filed against him by Company B in the e-QIP he completed in April 2014. But he denied any deliberate omission and claimed his omission of the Company B lawsuit was the result of a mistake, not falsification. He claimed the lawsuit was concluded more than three years prior to his completing his e-QIP and his erroneous

omission was an isolated incident on the form that was otherwise thorough and accurate in all other respects.

Findings of Fact

Applicant is a 34-year-old director of business development for a defense contractor who seeks a security clearance. The allegations covered in the SOR were denied by Applicant and placed in issue. Findings follow.

Background

Applicant immigrated to the United States in February 1994 as an Indian citizen and recent refugee from Nigeria. (GE 1; Tr. 35), and he became a naturalized U.S. citizen in November 2010. (GE 1) He married in March 2011 and reported no divorce or formal separation from his spouse. Since January 2012, he has resided with his parents, and the status of his marriage is unclear. (GE 1) Applicant has no reported children from his marriage. (GE 1)

Applicant earned a bachelor of science degree in engineering in May 2003 and a master of science degree in June 2004 from recognized U.S. universities. (GE 1) He claimed no military service or legal training. (GE 1; Tr. 50-51)

Applicant has worked for his current employer (Company A) since March 2006 as a director of business development. (GEs 1-2 and 5; Tr. 32, 40) Between January 2004 and March 2006, he worked as a vice president of business development for another firm. (GE 1) Applicant has held a security clearance since 2008 with DOD (upgraded to top secret according to Applicant) and a separate clearance since 2009 with an intelligence agency. (Tr. 36) He is familiar with the importance of providing the information requested in security clearance applications. (GE 1; Tr. 35)

Applicant's Software Licensing Initiatives

Company B is a software competitor of Company A that similarly develops analysis software that it sold to the intelligence, defense, and law enforcement communities. (GEs 2 and 5) Company A's marketing materials promote its software as a program generated from the start-up's developed methodology for combating fraud. (GEs 2 and 5) Shortly after joining Company A, Applicant contacted Company B about purchasing Company B products for Company C and furnished Company B his personal email address. (GEs 2, 5; Tr. 43-44) Applicant, in turn, purchased software from Company B using his father's credit card under the guise of purchasing the software for his father's company (Company C). (Tr. 45-46) Because he did not want Company B (an active competitor) to know he worked for Company A, he did not give Company B his business address at Company A. (Tr. 45)

Applicant was an employee of Company C between 2004 and 2009. He is no longer associated with the company. Company C is a company set up by Applicant's

father prior to 2004. Applicant was interested in Company B products that could be used for commercial fraud purposes. (GEs 2 and 5; Tr. 45-46)

In April 2006, Applicant, operating through Company C, purchased a proprietary software development kit and related technical support from Company B. At the time of the purchase, Applicant was Company A's director of business development and also an employee of Company C. (GEs 2 and 5 an AE A) When Company B asked for more information about Company C, Applicant furnished Company C's registered address in another state. (GEs 2 and 5) The proprietary software purchased from Company B offered Company A's customers a way to import the customers' data into Company A's products. Applicant used his father's credit card to pay for the licensing of Company B's software.

Company A is a software developer that sells certain of its analysis software to intelligence, defense, and law enforcement agencies, and assists these departments and agencies in their missions of solving counter terrorism problems. (Tr. 34-35) Company A clients include both private commercial companies and Government departments and agencies (approximately 90% commercial-related and roughly 10% Government-related). (Tr. 33-34, 39) The software employed by Company A is designed to facilitate the easy integration of disparate silos of data, whether globally or domestically situated. (Tr. 34)

In its business pursuits, Company A competes directly with Company B with respect to the sale of certain products. (GEs 2 and 5; Tr. 33) Applicant's father was a managing partner of Company C prior to August 2010, and his brother worked for Company C as a summer intern providing engineering input and is a member of Company C. (GEs 2 and 5)

While employed by Company A, Applicant registered for and attended a portion of a Company B user conference. (GEs 2 and 5) During his attendance at this conference, in or around May 2006, he provided his home address and mobile phone number, and identified his company as Company C.

In January 2007, Company B sold Applicant's father and Company C a license to Company's B's X designer software, along with one year of technical support. (GE 5; Tr. 46) In August 2007, Applicant contacted Company B and requested by email that certain software items be consolidated, and used his father's name as the requester. (GEs 2 and 5) Between January 2007 and August 2010, Applicant continued to acquire Company B software for Company A's business use, using his father and his Company C firm as the purchasing agent.

In August 2010, Company B filed a civil complaint in federal court against Companies A and C and named Applicant, his father, and other interested parties in the suit. (GE 2) In its complaint, Company B alleged a multiple scheme of fraudulent industrial espionage and broke its claims down into counts of contract and copyright breach, fraudulent conspiracy, misappropriation of trade secrets, and civil claims covered by the federal statute (18 U.S.C. § 1962(c), entitled the Racketeer Influence and Corrupt

Practices Act (RICO). (GE 2) Applicant and the other named defendants answered the complaint individually between August 2010 and October 2010. (GEs 3-5) Whether the parties engaged in any discovery before settling their lawsuit is unknown. Because Applicant and the other defendants denied most of the charging allegations, little of the specifics is known about the respective roles played by the individual defendants in the alleged multi-year fraud scheme directed at Company B.

Summarized, Applicant worked with his father and others at Company A in establishing Company C in early 2006 as an instrument of Company A. The founders designed Company C for the purpose of contacting and arranging for the licensing of proprietary intelligence analysis software and technical support for the use and licensing by Company A (a competitor of Company B) to its own employees and for re-licensing to customers of Company B. Applicant's designated role was to contact Company B and arrange for the purchase of its proprietary software and technical support without disclosing Company A's close relationship with Company C. (Tr. 43-45) These inter-relationships are well supported by the pleadings and evidence in the record.

At the time of Company C's acquired licensing of Company B's software in March 2006, Company A and Company C had interlocking directors and operated as a single entity when contracting with Company B for its proprietary software. Applicant as a director of both Company A and Company C was instrumental in making contact with Company B and arranging for the licensing of Company B's software without identifying his own relationship with Company A and his family's controlling interests in both companies.

In February 2011, Company A and Company C settled their lawsuit with Company B. Their settlement resolved multiple claims and counterclaims between the parties. (GEs 2 and 5; Tr. 49) More specifically, the parties' settlement resolved Company B's multiple claims against Company A and Company C for, *inter alia*, breach of contract and copyright, misappropriation of trade secrets included in Company B's proprietary software, and engagement in industrial espionage. Under the terms of the parties' settlement, Company A paid Company B the sum of $11 million in damages and removed all import features of Company B's software.

Although the evidence is lacking in proving any misappropriation of Company B's proprietary software by Company A, or any of its corporate or individual agents and affiliates, inferences are warranted that Applicant played a major role in the contacting and arranging for Company A's licensing of Company B's proprietary software through Company C without disclosing the close relationships he and Company C shared with Company A, a direct competitor of Company B and an unlikely partner with Company A on any mutual software licensing agreement.

Applicant characterized his actions in arranging the purchase of Company B proprietary software as a youthful mistake. (GE 5; Tr. 44) His admitted actions, while not fully developed, do not reflect youthful mistakes by a 24-year-old, highly educated engineer. To the contrary, his actions represent concerted attempts to obtain software

and technical support by surreptitious means that he knew at the time was wrong. (Tr. 41, 48-49) By holding himself out as a representative of Company C in purchasing Company B's software, he concealed his role as a director of Company A, the real party in interest in buying Company B's software and technical support.

Applicant claimed his noble goals of saving lives by merging Company B's software with Company's A's to create the desired effect of information inseparability. He considered these goals to be justification enough for utilizing fraudulent means to acquire Company B's software. With this justification for moving forward, he elevated important security ends over lawful means to complete his purchases. Noble or not in his overall thinking, Applicant's actions were undertaken with the intent to mislead and defraud Company B into releasing its proprietary software and were undertaken dishonestly for self-serving purposes. He offered no good reasons that he could not have used lawful business practices to obtain needed software from Company B.

Applicant's E-QIP Omissions

Asked to complete an e-QIP in April 2014, Applicant omitted his being named as a party in a Company B lawsuit filed in 2010, along with, *inter alia,* Companies A and C. (GE 1) Applicant denied any deliberate omission of the lawsuit and claimed his omission was the result of a mistake of what he characterized as a minor omission of a major lawsuit. (GE1; Tr. 37-38) To be weighed in determining whether Applicant's denial is credible are his educational background; his deep knowledge of information technology systems and their proprietary features that offer interoperability opportunities; his extensive experience in the marketing of intelligence-related software world-wide; and his familiarity with the issues and importance of the Company B lawsuit.

In answering his 2014 e-QIP, Applicant claimed to mistakenly contextualize the section 28 question differently, interpreting the question to encompass the named companies (i.e., Companies A-C) in the lawsuit, and not the named individuals like Applicant. (Tr. 37, 41) The question inquiring about prior lawsuits in which Applicant was a named party is straightforward and asks specific information about being named in a lawsuit that he answered in 2010.

Motivation for his omitting the lawsuit information in his e-QIP was considerable given his recent history of intentionally withholding his real interests from Company B to maximize his chances of his completing software purchases with Company B. Applicant's e-QIP omission reflects some pattern of according a higher priority to his personal interests when faced with conflicting choices of withholding and disclosure.

Applicant was apparently never interviewed by an agent of the Office of Personnel Management (OPM) following his submission of his e-QIP. Claiming his first opportunity to review allegations of falsification of his e-QIP came after he received the SOR in September 2015, he admitted the lawsuit in his SOR response. Applicant's claims cannot be easily reconciled, though, with his statement that he believed the lawsuit was of a commercial nature that primarily concerned Companies A and B. The question asked of

him was neither complicated nor ambiguous, and he was well aware at the time he answered the question that he was a named party to the lawsuit filed by Company B and filed a detailed answer to the complaint through his retained attorneys.

Considering all of the circumstances surrounding Applicant's omission of the 2010 Company B civil lawsuit naming him, along with his company and family affiliations, his falsification denials cannot be reconciled with his e-QIP omission. Applicant is highly educated in the field of engineering, is well-traveled in marketing his company's software (GE 1), and has considerable familiarity with not only the technical features of intelligence software, but the demanding disclosure requirements imposed on applicants who apply for a security clearance. Without more direct evidence of Applicant's intentions when answering section 28 of the e-QIP he was asked to complete, drawn inferences of knowing and wilful omission cannot be averted.

Endorsements

Applicant is well-regarded by Company A's president (President X). (AE C) In his declaration of March 2016, President X confirmed his overall responsibility for the security of classified information held by Company A and for building the back-end software layer that powers Company A's government platform. He confirmed his working relationship with Applicant since early 2006 and offered praise for Applicant's conscientious work in behalf of their Government counterparts. (AE C)

President X recited his facility clearance officer (FSO) role at Company A when applicant applied for and received his original security clearance and subsequent additional eligibility levels. (AE C) Based on his work with Applicant over a number of years, President X characterized Applicant as reliable, trustworthy, and serious about protecting the information that he and Company A were entrusted with. (AE C) He made no mention, however, of his familiarity with the Company B lawsuit or Applicant's involvement in Company B's software program. (AE C)

Consultants who worked with Applicant while tasked to provide security assistance to Company A expressed praise for his joint efforts in securing a facility clearance for the firm in 2007 and in building Company A's security program. (AE A) Consultant K credited Applicant with displaying the highest moral and ethical characteristics for others to emulate and with showing the utmost respect for the Government and the sensitive information with which he is entrusted. (AE A) Consultant K expressed no familiarity with the Company B lawsuit or any Applicant involvement in Company B's software program. (AE A)

Co-workers with strong military backgrounds who have worked closely with Applicant extolled his exhibited dedication to U.S. security interests and unquestioned loyalty and trust. (AE B) Co-worker P cited his observations of Applicant's implementation of plans, procedures, and training to ensure the company was in compliance with Government guidance on classified material. Co-worker P always found Applicant to be completely reliable and trustworthy "as much as anyone I went to combat with." (AE B) His

co-workers expressed no familiarity with the Company B lawsuit or any Applicant involvement in Company B's software program. (AE B)

Policies

The AGs list guidelines to be used by administrative judges in the decision-making process covering security clearance cases. These guidelines take into account factors that could create a potential conflict of interest for the individual applicant, as well as considerations that could affect the individual's reliability, trustworthiness, and ability to protect classified information. These guidelines include "[c]onditions that could raise a security concern and may be disqualifying" (disqualifying conditions), if any, and many of the "[c]onditions that could mitigate security concerns." Each of these conditions must be considered before deciding whether or not a security clearance should be granted, continued, or denied. The guidelines do not require administrative judges to place exclusive reliance on the enumerated disqualifying and mitigating conditions in the guidelines in arriving at a decision. Each of the guidelines is to be evaluated in the context of the whole person in accordance with AG ¶ 2(c)

In addition to the relevant AGs, administrative judges must take into account the pertinent considerations for assessing extenuation and mitigation set forth in AG ¶ 2(a) of the AGs, which are intended to assist the judges in reaching a fair and impartial commonsense decision based upon a careful consideration of the pertinent guidelines within the context of the whole person. The adjudicative process is designed to examine a sufficient period of an applicant's life to enable predictive judgments to be made about whether the applicant is an acceptable security risk.

The following AG ¶ 2(a) factors are pertinent: (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 chances; (7) the motivation for the conduct; (8) the potential for pressure, coercion, exploitation, or duress; and (9) the likelihood of continuation or recurrence.

Viewing the issues raised and evidence as a whole, the following individual guidelines are pertinent in this case:

Personal Conduct

The Concern: Conduct involving questionable judgment, untrustworthiness, unreliability, 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. AG, ¶ 15.

Burden of Proof

By virtue of the principles and policies framed by the AGs, a decision to grant or continue an applicant's security clearance may be made only upon a threshold finding that to do so is clearly consistent with the national interest. Because the Directive requires administrative judges to make a commonsense appraisal of the evidence accumulated in the record, the ultimate determination of an applicant's eligibility for a security clearance depends, in large part, on the relevance and materiality of that evidence. *See United States, v. Gaudin,* 515 U.S. 506, 509-511 (1995). As with all adversarial proceedings, the judge may draw only those inferences which have a reasonable and logical basis from the evidence of record. Conversely, the judge cannot draw factual inferences that are grounded on speculation or conjecture.

The Government's initial burden is twofold: (1) it must prove by substantial evidence any controverted facts alleged in the SOR, and (2) it must demonstrate that the facts proven have a material bearing to the applicant's eligibility to obtain or maintain a security clearance. The required materiality showing, however, does not require the Government to affirmatively demonstrate that the applicant has actually mishandled or abused classified information before it can deny or revoke a security clearance. Rather, the judge must consider and weigh the cognizable risks that an applicant may deliberately or inadvertently fail to safeguard classified information.

Once the Government meets its initial burden of proof of establishing admitted or controverted facts, the evidentiary burden shifts to the applicant for the purpose of establishing his or her security worthiness through evidence of refutation, extenuation, or mitigation. Based on the requirement of Exec. Or. 10865 that all security clearances be clearly consistent with the national interest, the applicant has the ultimate burden of demonstrating his or her clearance eligibility. "[S]ecurity-clearance determinations should err, if they must, on the side of denials." *See Department of the Navy v. Egan,* 484 U.S. 518, 531 (1988).

Analysis

Security concerns are raised over Applicant's active role in the purchasing of proprietary software on behalf of a company controlled by the competitor of the firm he was actively seeking to acquire sensitive proprietary software from. This seller later filed a lawsuit naming Applicant, his companies, and others in a conspiracy to misappropriate the licensing company's copyrights and trade secrets.

Additional security concerns are raised over Applicant's material omission of the Company B lawsuit in the e-QIP he completed in April 2014. His claims of mistake in his omission of the lawsuit are not supported by evidence of a good-faith misreading of the plain language of the section 28 inquiry contained in applicant's e-QIP.

Proprietary Software Misappropriation Concerns

Historically, settlements of civil lawsuits are not admitted to prove facts alleged in the pleadings, and which are not proven by competent and admissible evidence. *See United States v. Bailey*, 696 F.3d 794, 801 (9th Cir. 2012). Settlement agreements are barred from admission to prove the validity or validating of a claim or its amount. *See* Rule 408 of Fed. R. Evid. However, Rule 408 does not preclude the admission of facts covered in settlement agreements or elsewhere in the record. Pleading admissions unrelated to settlement discussions or agreements fall with the Rule's exceptions

Applicant's pleading admissions with respect to his relationships with Companies A and C, his role in contacting and arranging for purchases of Company B's proprietary software on multiple occasions between 2006 and 2010, and his approval of the ensuing Company A settlement of the Company B lawsuit that included a Company A payment of $11 million in damages to Company B and removal of Company B's software from Company A's software programs are well-established and negate the need for any independent proof. *See McCormick on Evidence,* § 262 (6th ed. 2006).

Because Applicant's pleading admissions did not include details of his purchases and uses of Company B software as an undisclosed intermediary for Company A in arranging for the purchases of Company B software, additional evidence was needed to tie-in Applicant to Company B's multiple claims of fraud, contractual breaches, misappropriation of Company B trade secrets, copyright infringement, and civil RICO violations. Applicant supplied that missing information at hearing with his own testimony at hearing.

Applicant's admissions include acknowledgments of his (a) surreptitious use of Company C for purchases of Company B proprietary software to conceal his connections with Company A, the real party in interest and close competitor of Company B, (b) his use of his father's credit card to complete his Company B software purchases, and (c) his naming as a material defendant in the Company B lawsuit, and (d) his approval of the Company A and Company C settlement with Company B. Applicant's pleading and evidentiary admissions when considered in their entirety reflect dishonest conduct and serious judgment lapses that cast doubt on Applicant's worthiness to hold a security clearance.

Taking into account all of the facts and circumstances presented in the record, inclusive of Applicant's admissions, the SOR allegations that attribute wrongful participation by Applicant and others in a multi-year scheme of fraud and industrial espionage by operating as a representative of a shell company (Company C) to obtain software from Company B for other Company A employees and Company B customers are well demonstrated. Pleading and evidentiary admissions support drawn inferences that Applicant and other Company A employees incorporated Company B's proprietary

software in Company A's platform to achieve the desired interoperability to maximize the data Company A supplied its government customers.

Based on the foregoing findings and conclusions, DC ¶ 16(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 protected information;

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

(4) evidence of significant misuse of Government or other employer's time or resources. . . ."

While the evidence is less than clear how much Applicant's role in misusing Company A's resources to acquire Company B software by surreptitious means and pass it on to both Company B's customers and Company A's employees and customers by fraud and concealment, his contributions to Company A's illicit software acquisitions from Company B were considerable and reflect a material role in Company A's fraudulent scheme in acquiring Company B's proprietary software over an extended period of years.

Mitigation is lacking in Applicant's proofs. His characterizing his actions as youthful mistakes are unconvincing when evaluating his claims against his record of superior educational achievements with respected universities and his years of working with sophisticated software and technical services. (GE 1) Not only are his misleading enticements with Company B highly material to an overall trustworthiness assessment, but his indiscretions reflect still recent pattern acts of dishonesty that pose risks of recurrence. Positive steps to reduce or eliminate risks of recurrence are not in evidence. Considering all of the evidence presented, mitigating conditions are not available to Applicant.

e-QIP Omission Concerns

In the process of completing an e-QIP in April 2014, Applicant failed to disclose his being named as a defendant in a suit filed by Company B in 2010. Applicant's claims and explanations about his mistaken interpretation of the question covered by section

28 of his e-QIP are not credible. Both motive and past history of withholding his Company A business relationship when dealing with Company B provide ample reasons for his intentionally withholding disclosure of the Company B lawsuit in his e-QIP. Considered together under all of the facts and circumstances presented, Applicant's lawsuit omission reflects knowing and wilful conduct that raises security additional concerns under Guideline E.

One of the disqualifying conditions covered by Guideline E are applicable. DC ¶ 16(a), "deliberate omission, concealment, or falsification of relevant facts to 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." DC ¶ 16(a) may be considered in evaluating Applicant's e-QIP omission of Company B's 2010 civil lawsuit filed against himself, Companies A and C, and other family members and associates.

Traditional assessments of falsification in ISCR proceedings include considerations of motive in determining whether particular applicants engaged in knowing and willful concealment. Both Guideline E and relevant case authorities underscore the importance of motive and subjective intent considerations in gauging knowing and willful behavior. *See* ISCR Case No. 03-10380 at 5 (App. Bd. Jan. 6, 2006)(citing ISCR Case No. 02-23133 (App. Bd. June 9, 2004)). *See, generally*, *United States v. Chapin,* 515 F.2d 1274, 1283-84 (D.C. Cir. 1975); *United States v. Steinhilber*, 484 F.2d 386, 389-90 (8th Cir. 1973); *United States v. Diogo*, 320 F.2d 898, 905 (2d Cir. 1963). Put differently, the Government must be able to negate any reasonable interpretation that will make Applicant's explanations about his lawsuit omission in his e-QIP factually justifiable. Use of a subjective intent test is not intended to straightjacket either party with particular words and phrases, but rather to avert definitional traps.

Potential mitigating conditions are not available to Applicant under the facts of this case. Not until he was confronted with the SOR in September 2015 did he acknowledge his Company B lawsuit omission and offer explanations of mistake and misunderstanding of the question. By this time, DOD investigative resources had already discovered the existence of the lawsuit naming, *inter alia,* Applicant as a defendant.

In evaluating all of the circumstances surrounding Applicant's intentional withholding of material information about his involvement in a major and material lawsuit in the e-QIP he completed, his explanations and timing of his corrections are insufficient to convincingly refute and mitigate the deliberate falsification allegations. Questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations, are each core policy concerns of the personal conduct guideline (AG ¶ 15),

which have been compromised by Applicant in repeated instances in this case. Imputed acts of Applicant dishonesty and judgment lapses in this case are not mitigated.

From a whole-person standpoint, there is considerable evidence favoring Applicant from his company president, consultants, and co-workers. Each of his references places a high value on his contributions and adherence to safeguarding classified and sensitive information. Judgment and trust issues associated with his withholding material information from his Company B software supplier about his interests in Company A (a major competitor of Company B) and his ensuing falsification of his 2014 e-QIP by withholding his involvement in Company B's lawsuit cannot be reconciled with principles of honesty, trust, and good judgment. Overall, Applicant is not able to demonstrate with his proofs that he possesses the level of trustworthiness, reliability, and good judgment necessary to meet security eligibility requirements.

In making a whole-person assessment, careful consideration was given to the respective burdens of proof established in *Egan* (*supra*), the AGs, and the facts and circumstances of this case in the context of the whole person. Unfavorable conclusions warrant with respect to the allegations covered by subparagraph 1.a and 1.b.

Formal Findings

In reviewing the allegations of the SOR and ensuing conclusions reached in the context of the findings of fact, conclusions, conditions, and the factors listed above, I make the following formal findings:

GUIDELINE E (PERSONAL CONDUCT): AGAINST APPLICANT

Subparas. 1.a-1b:	Against Applicant

Conclusions

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

Roger C. Wesley
Administrative Judge