DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 11-00180
	)	
Applicant for Security Clearance	)	

Appearances

For Government: David Hayes, Esquire, Department Counsel
For Applicant: John V. Berry, Esquire

01/03/2013

Remand Decision

ANTHONY, Joan Caton, Administrative Judge:

After a thorough review of all evidence in the record of this case, and after carefully observing Applicant and assessing his demeanor and credibility, I conclude that Applicant failed to mitigate the Government's security concerns under Guideline E, Personal Conduct. His eligibility for a security clearance is denied.

Statement of the Case

As the employee of a defense contractor, Applicant completed and signed an Electronic Questionnaire for Investigations Processing (e-QIP) on April 15, 2010. In September 2010, he was interviewed about a civil court action by an authorized investigator from the U.S. Office of Personnel Management (OPM). On July 27, 2011, Applicant provided notarized responses to interrogatories posed by the Defense Office of Hearings and Appeals (DOHA). On September 29, 2011, DOHA issued Applicant a Statement of Reasons (SOR) detailing security concerns under Guideline E, Personal Conduct, and Guideline F, Financial Considerations. DOHA acted 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 for SORs issued after September 1, 2006.

On October 18, 2011, Applicant answered the SOR in writing and elected to have a hearing before an administrative judge. The case was assigned to me on November 29, 2011. I convened a hearing on January 6, 2012, to consider whether it is clearly consistent with the national interest to grant or continue a security clearance for Applicant. The Government called no witnesses, introduced two exhibits, and offered facts in two compilations of state code citations for administrative notice. The Government's exhibits were marked as Exhibit (Ex.) 1 and Ex. 2 and entered in the record without objection.[1] Applicant did not object to notice of the facts in the documents offered for administrative notice, which were marked as Hearing Exhibit (HE) 1 and HE 2 and included in the record without objection. Applicant testified on his own behalf, called two witnesses, and offered 15 exhibits, which were marked as Ex. A through Ex. O and admitted to the record without objection. DOHA received the transcript (Tr. 1) of the hearing on January 10, 2012.

On March 8, 2012, I issued a decision denying Applicant a security clearance. My decision found that Applicant mitigated financial considerations security concerns alleged in the SOR, but he failed to mitigate security concerns under the personal conduct adjudicative guideline. On June 19, 2012, DOHA's Appeal Board remanded my decision for further action, noting that the doctrine of collateral estoppel was not appropriately applied in my decision and, accordingly, Applicant should be permitted to submit additional information that might clarify and mitigate the conduct alleged in the SOR.

At the direction of the Appeal Board, I convened a hearing on September 26, 2012, to consider new evidence from Applicant's civil trial regarding his underlying conduct. The new evidence included civil trial pleadings, direct and cross-examination testimony of Applicant, testimony of a computer forensic expert, the parties' closing arguments, and the jury verdict form. Additional evidence considered included Applicant's employment agreement, his position of trust letter, and the opinion of the state Supreme Court, affirming in part, reversing in part, and remanding the verdict of the trial court in the civil proceeding against Applicant and other defendants.

The Government called no witnesses and introduced eight exhibits, which were marked as Government exhibits (Ex.) 1 through Ex. 8 and entered in the record without

[1] For consistency and clarity, the exhibits entered in the record at the January 6, 2012, hearing are identified as follows: for the Government: Ex. 1-1 and 1-2; and for Applicant: Ex. 1-A through 1-O. The transcript of the January 6, 2012 hearing is identified as Tr. 1.

objection.[2] Applicant testified, called two additional witnesses, and introduced six exhibits, which were marked as Applicant's exhibits (Ex.) A through Ex. F and entered in the record without objection. At the conclusion of the hearing, I left the record open until close of business October 10, 2012, so that additional documentation could be provided for the record. The Government introduced two additional exhibits, Ex. 9 and Ex. 10, which were entered in the record without objection. Applicant introduced one additional exhibit, which was marked as Ex. G and entered in the record without objection. DOHA received the second transcript (Tr. 2) on October 16, 2012.

Findings of Fact

The previous decision in this matter, including all testimony and exhibits, is incorporated in this remand decision by reference. Additionally, after careful review of the exhibits submitted and the testimony offered by the parties at the September 26, 2012 hearing. I make the following findings of fact:

Applicant is 55 years old, married, and the father of two adult daughters. He is employed as a senior program manager by a government contractor. A high school graduate, he enlisted in the military in 1976. He rose to the highest levels of the enlisted ranks and was subsequently commissioned as an officer, a position in which he also excelled. He retired from the military in 2000, and he received an honorable discharge. He held security clearances during his military service and as a civilian contractor. (Ex. 1-1; Ex. 1-2; Ex.1- A; Tr. 1: 63-67, 86, 112.)

In 2000, after his military retirement, Applicant went to work for a small technology company. As an employee of the technology company, Applicant, on July 17, 2000, signed the following position of trust letter provided to him by his employer:

> In the course of carrying out your duties and responsibilities as an employee of [name of company] you may have access to sources of sensitive, company-private and/or personnel and financial information and data (hereafter referred to as data). [Name of company] trusts you to use this data appropriately. The data, wherever and however derived, is for official use only in the performance of your assigned duties. You have the direct responsibility of protecting this data from unauthorized disclosure. You are not to make this data available in any form to any unauthorized person, company or entity without prior written approval of [the company's] President. Any violation of the Trust could subject you to immediate dismissal without recourse and without severance pay.

[2] Again, for consistency and clarity, exhibits entered in the record at the remand hearing are further identified as follows: for the Government: Ex. 2-1 through Ex. 2-10; and for Applicant: Ex. 2-A through 2-G.

> I understand the sensitivity of the Position of Trust to which I am assigned and the severity of the penalty for any violation of such trust. (Ex. 2-3.)

As the employee of the small technology company, Applicant also signed an employment agreement, which contained a nondisclosure admonition, specified at paragraph VI:

> In the course of his/her employment, Employee will have access to Company confidential records, data, formulae, specifications, customer lists, personnel records, financial information and personal information owned by [name of company] and used in the course of its business. During his/her employment by [name of company] and thereafter, Employee will not directly or indirectly disclose or use any such information except as required in the course of [name of company] employment. Unauthorized disclosure of any such information may result in termination for cause. All records, files, drawings, documents, equipment and the like, relating to [name of company's] business which Employee shall prepare or use [or] will come into contact with, shall remain [name of company's] sole property and shall be promptly returned to [name of company] in the event of dismissal or termination of employment by either [name of company] or the Employee. (Ex. 2-3.)

At his remand hearing, Applicant stated that he did not believe the nondisclosure agreement applied to him when he was an employee of Company A. He said he concluded this because he thought the presiding judge at his civil trial ruled that it was not transferable and it was too broad. However, the jury in his civil trial found that the nondisclosure agreement provisions did apply to Applicant during his tenure at Company A. This finding was not addressed by the final amended order of the trial court, and it was not overturned by the state supreme court. (Ex. 1-2; Ex. 2-8; Tr. 2: 111-114.)

Paragraph VIII of the employment agreement that Applicant signed also stated:

> This Agreement shall not be terminated by the voluntary or involuntary dissolution of [name of company] or by any merger or consolidation where [name of company] is not the surviving or resulting corporation, or upon any transfer of all or substantially all of the assets of [name of company]. In the event of any such merger or consolidation or transfer of assets, the provisions of this Agreement shall be binding on and shall insure to the benefit of the surviving or resulting corporation or the corporation to which such assets shall be transferred. (Ex. 2-3.)

On April 2, 2001, Applicant also signed the company's electronic media acknowledgement form, which provided as follows:

> As an employee of [name of company], I have read the Company policy regarding use of Company provided electronic media and services. I recognize and understand that all electronic media and services such as computers, e-mail, telephones, voice mail, fax machines and the Internet, are the property of [name of company] and are to be used for conducting the Company's business only. I understand that limited, occasional, or incidental use of electronic media (sending or receiving) for a personal purpose is permitted, but must not interfere with my productivity, the productivity or rights of other [company] employees, or the business of the company. Further, I understand that the Company has the ability to monitor and access my use of these systems and services and that the Company can override any password for the purpose of system security. I agree not to access a file or retrieve any stored communication other than where authorized unless there has been a prior clearance by the authorized Company representative.
>
> I am aware that the Company reserves and will exercise the right to review, audit, intercept, access and disclose all matters on the Company's electronic media and services at any time, with or without employee notice, and that such access may occur during or after working hours. I am aware that the use of Company-provided passwords or codes does not restrict the Company's right to access electronic media. I waive the right to assert claims of invasion of privacy or any other claims arising out of or pertaining to the use of electronic media against [name of company]. I am aware that violations of this policy may subject me to disciplinary action up to and including termination of employment. (Ex. 2-2.)

The small technology company was purchased between 2000 and 2001 by Company A, a defense contractor. Applicant continued to work as a manager and supervisor at Company A until 2009. As an employee of Company A, Applicant did not sign a new nondisclosure agreement. (Ex. 1-1; Tr.1: 70.)

In his work at Company A, Applicant directed the work of between 30 and 35 employees who were program managers. There came a time when Applicant became aware of morale problems at Company A. Employees were not able to receive bonuses, and the company reduced its contributions to employee retirement accounts. A larger business was considering the purchase of Company A. A number of employees left Company A and sought employment elsewhere.[3] (Tr. 1: 67, 105.)

Applicant learned that a former colleague and friend in Company A, who had left Company A in January 2008, was establishing a government services division at Company B, another government contractor. Another individual, also a personal friend

[3] Applicant estimated that of the 250 employees in the work group at Company A, 50 to 75 left for other positions during this time. (Tr.1: 103.)

of Applicant's and a former colleague at Company A, was in a leadership position at Company B.[4] Additionally, Applicant was the direct supervisor of still another individual who left Company A and accepted employment at Company B. Applicant and several individuals in this group had met and served together in the military. As government contractors, they worked on projects they had become familiar with during their military service. (Ex. 1-1; Ex. 2-6; Tr. 1: 81-82, 116-118, 135, 145-149; Tr. 2: 152-155, 216-222.)

In May 2009, Applicant sent his resume to his former colleague and old friend, the individual establishing the government services division at Company B. The individual responded by sending Applicant an offer of employment, which Applicant accepted. Applicant was also a friend of the individual who was hired to recruit and fill other positions at Company B. This individual expressed interest in hiring Applicant's deputy. Applicant provided him with his deputy's telephone number. Applicant also attended a lunch with his deputy and an official at Company B, but he stated that he was not present when discussion of his deputy's possible employment with Company B occurred. However, the Company B official sent Applicant a proposed benefits package for his deputy and asked him to transmit it to him. Applicant and the Company B officials denied an intent to actively recruit, poach, or "raid" Company A employees. (Tr. 1: 134-135; Tr. 2:103-112, 161-165, 178-185.)

Applicant resigned from Company A on June 5, 2009. At an exit interview, he returned to an official of the company the following equipment provided him by his employer: a blackberry, two cell phones, a pager, and one computer. He also handed over his iPhone provided by the employer to the individual he thought would succeed him as program director. He signed a statement, provided by his employer, acknowledging that he had returned all property belonging to the employer, and he had not retained

> any, property and information belonging to [Company A] and/or relating to [Company A's] business, including but not limited to [Company A]-issued computers, hand-held and other electronic devices; project and customer information; financial and accounting information; information concerning [Company A] employees; and all other tangible and intangible property, documents, files and other information belonging to, or relating to the business of [Company A]. (Ex. 2-4.)

In an interview with an authorized investigator from the Office of Personnel Management in September 2010, Applicant stated that when he left his job with Company A, he took with him a personal 20 gigabyte hard drive. At his January 6, 2012 hearing, Applicant testified that he took with him his personal 20 gigabyte hard drive, which he had used while employed for nine years at Company A. Applicant stated that he used the personal hard drive because the equipment provided by his employer

[4] This individual left Company A around 2004. He later served as an Assistant Secretary in the Executive Branch of the U.S. Government. (Ex. 1-B; Tr.1: 81-82, 101-102.)

lacked sufficient memory to store the information he wished to archive. He explained that he used the hard drive to store pictures, family data, recipes, and archived e-mails. He stated that there were also some power point presentations belonging to Company A on his hard drive. He put the hard drive in the trunk of his automobile when he left Company A. Later, on the advice of counsel, he turned the hard drive over to Company A for forensic examination. Applicant stated that the forensic examination revealed that there was no classified information on his personal hard drive. (Ex.1-2; Tr.1: 70.)

Applicant claimed that he left Company A on good terms. He was responsible for directing two large programs serving military clients. He asserted that he appropriately transferred his duties to other managers and sent a farewell e-mail to those employees who reported to him. (Tr.1: 70-71.)

In late June 2009, within two weeks of assuming his new position at Company B, Applicant and the three other former senior employees of Company A were named as defendants, along with Company B, in a civil complaint brought against them by Company A. Company B retained counsel, which represented the company, Applicant, and the other three defendants. (Ex. 1-2; Tr.1: 68, 87.)

The civil complaint alleged that Applicant had breached his fiduciary duty to Company A and breached his employment contract (non-disclosure agreement) with Company A. The civil complaint also alleged that Applicant violated a state computer crimes act and that he, along with the other named defendants, violated a state business conspiracy act. Additionally, the civil complaint alleged that Applicant and his co-defendants were liable on a claim for civil conspiracy and that Applicant was liable on claims of misappropriation of trade secrets and conversion. (Ex. 1-2.)

I take administrative notice of the applicable state uniform trade secrets act, which defines “misappropriation” as follows:

1. Acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or

2. Disclosure or use of a trade secret of another without express or implied consent by a person who

a. Used improper means to acquire knowledge of the trade secret; or

b. At the time of disclosure or use, knew or had reason to know that his knowledge of the trade secret was

(1) Derived from or through a person who had used improper means to acquire it;

(2) Acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use;

(3) Derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or

(4) Acquired by accident or mistake. (HE 1)

The state statute defines "improper means" to include "theft, bribery, misrepresentation, use of a computer or computer network without authority, breach of a duty or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means." (HE 1)

The state statute further states: "If willful and malicious misappropriation exists, the court may award punitive damages in an amount not exceeding twice any award made under subsection A of this section [specifying terms for money recovery of damages] or $350,000 whichever amount is less." Additionally, the statute provides: "If the court determines that (i) a claim of misappropriation is made in bad faith, or (ii) willful and malicious misappropriation exists, the court may award reasonable attorneys' fees to the prevailing party." (HE 1)

I also take administrative notice of the applicable state business conspiracy act, which reads, in pertinent part:

> A. Any two or more persons who combine, associate, agree, mutually undertake or concert together for the purpose of (i) willfully and maliciously injuring another in his reputation, trade, business or profession by any means whatever or (ii) willfully and maliciously compelling another to do or perform any act against his will, or preventing or hindering another from doing or performing any lawful act, shall be jointly and severally guilty of a Class 1 misdemeanor. Such punishment shall be in addition to any civil relief recoverable under [Code citation omitted].
>
> B. Any person who attempts to procure the participation, cooperation, agreement or other assistance of any one or more persons to enter into any combination, association, agreement, mutual understanding or concert prohibited in subsection A of this section shall be guilty of a violation of this section and subject to the same penalties set out in subsection A. (HE 2)

The statute defines "damages" to include loss of profits, and it authorizes recovery of treble damages and attorneys' fees upon a finding of willful and malicious injury by conspiracy to reputation, trade, business, or profession. (HE 2)

Applicant and his co-defendants were represented by counsel hired by Company B. During preparation for trial, Applicant met individually with counsel for several hours. In these pre-trial consultations, Applicant insisted that he had done nothing wrong. (Tr.1: 87-88.)

Applicant's case was tried in civil court before a jury. The trial ran for 11 days. At trial, Applicant was called to testify, and he did so for approximately 45 minutes. He was then cross-examined for approximately 20 minutes. His position remained that he had done nothing wrong.[5] (Tr.1: 87-90.)

At the trial, Applicant admitted that in the first half of 2009, he and his friend at Company B discussed gathering together a group of like-minded individuals to do government contracting work that would include projects similar to those carried out by Company A. The friend at Company B asked Applicant to identify individuals who would make good members of the new government contracts consulting group. Applicant told his deputy he was accepting a position with Company B. Applicant also told his friend at Company B that his deputy would be a good choice for the group being assembled. (Ex. 2-6.)

One Company A employee who learned of Applicant's intended move to Company B complimented him by saying that the work he did for Company A would follow him to Company B. After hearing this, Applicant sent an e-mail to his friend at Company B informing him of the compliment. (Ex. 2-6.)

Company A was planning to re-compete for a contract it held with the military. However, Applicant informed his friend at Company B that Company A had not developed a strategy to guide its proposal for the re-compete. Applicant assisted his friend at Company B in identifying Company A employees who might be recruited by Company B in submitting a competitive offer on the contract. On May 29, 2009, the Company B official sent an e-mail proposing June 4, 2009, as a date for several Company A employees to meet with him to discuss the re-compete contract. E-mails identified at trial by Applicant as either written by him or received by him demonstrated his active involvement in this activity. (Ex. 2-6.)

Also at the trial, a computer forensic expert called by plaintiff Company A testified that her analysis of Applicant's Company A computer revealed that on June 2, 2009, approximately three days before Applicant resigned from Company A to go to work at Company B, a 100-gigabyte hard drive had been attached to his computer and five folders created. One of the folders was labeled "Company B." A June 3, 2009, remote image analysis of the files on the 100-gigabyte hard drive and the files on Applicant's Company A computer revealed that several hundred files were copied from the company computer to the 100-gigabyte hard drive. The computer analysis also showed that once copied to the 100-gigabyte hard drive, the files were deleted from Applicant's computer and then also deleted from the computer's recycle bin.[6] Applicant acknowledged that he copied the files from his Company A computer to the 100-

[5] In colloquy with Department Counsel at his January 6, 2012 hearing, Applicant denied any wrongdoing as an employee of Company A and Company B. When asked by his counsel to explain the conduct involved in the claim of conversion, Applicant replied: "I don't even know what conversion is." (Tr. 1: 72, 85-86.)

[6] Applicant deleted a total of 1,400 files from his Company A recycle bin. (Ex. 2-B.)

gigabyte hard drive. A later analysis of Applicant's assigned computer at Company B did not reveal any of the files that Applicant had copied from his Company A computer to the 100-gigabyte hard drive. At the trial, it was alleged and established that the materials copied to the 100-gigabyte drive included Company A's proprietary information and trade secrets. It was also alleged and established that Applicant and the current and former employees of Company A and its predecessor company who went to Company B formed a core group of senior government contractors who planned to use information taken from Company A in order to compete for a lucrative government contract previously held by Company A. (Ex 2-5; Ex. 2-6; Ex. 2-B; Ex. 2-E; Tr. 2: 72-73,110-117.)

At his remand hearing, Applicant stated that on June 2, 2009, he had copied Company A material onto the 100-gigabyte hard drive to leave for the individual he believed would succeed him at Company A. Applicant testified that he placed the 100-gigabyte drive on his desk when he left Company A. The list of items Applicant returned to Company A when he left contains no mention of a 100-gigabyte drive. The individual Applicant identified as his successor at Company A was Applicant's deputy for several years. (Ex. 2-4; Tr. 2: 72-73.)

When Applicant left Company A, his deputy was on vacation. Applicant's former deputy at Company A appeared as a witness at the remand hearing and testified that at the end of May 2009, he submitted a letter of resignation to Company A in order to take a position, along with Applicant, at Company B. He further stated that he already had all the information he needed in order to assume duties as Applicant's successor, and he had no need for any Company A information that might have been placed on the 100-gigabyte drive. Applicant's former deputy also stated that he never received the 100-gigabyte hard drive. Applicant was unable to account for the whereabouts of the 100-gigabyte hard drive. (Tr. 2:126, 231-235.)

At his remand hearing, Applicant was reminded on cross-examination that at his January 6, 2012, DOHA hearing he had stated several times that he had done nothing wrong. Counsel then asked Applicant what his position was at the time of his remand hearing. Applicant replied:

> While, I would say my position today is I feel I did nothing wrong. I took a 20-gig hard drive. I didn't do any conversion. I didn't do anything. I didn't move anything to [Company B]. The drive I took with me is my own personal drive. I didn't think about what was on that drive. Not at all. Everything that I did at [Company A] was to further the job that [Company A], moving, you know, moving the 100 documents to the 100 hard drive was to, to help the program office. So, yes, I mean I've been found liable by the jury and have not been exonerated, in your words, but, you know, I still feel that I didn't move documents to [Company B]. I didn't conspire with anybody. I didn't poach people. I didn't do those things. (Tr. 2: 137.)

The civil jury found that Applicant was liable in money damages on the following claims: for breach of fiduciary duty, in the amount of $217,800, with an award of punitive damages of $217,800; for breach of contract (non-disclosure agreement), in the amount of $217,800; for violation of a state computer crimes act, in the amount of $217,800, with punitive damages of $217,800; for violation, along with the other named defendants, of a state business conspiracy act, in the amount of $12,341,535; for civil conspiracy, along with the other named defendants, in the amount of $4,113,845, with punitive damages of $12,341,535; for misappropriation of trade secrets, in the amount of $1,028,461, with punitive damages of $1,028,461; for conversion, in the amount of $12,920, with punitive damages of $25,840. (Ex. 2-7; Ex.1- 2.)

After the completion of the trial, both parties filed motions, and the circuit court judge reviewed the motions and the jury verdict. In October 2010, the judge entered final judgments against Applicant on the jury's findings. The final judgments ordered by the judge were as follows:

> Applicant, along with the other named defendants, jointly and severally, was ordered to pay damages of $12,341,535 for violations of the state business conspiracy act;
>
> Applicant was ordered to pay $350,000 in punitive damages awarded against him individually; and
>
> Applicant, along with the other names defendants, jointly and severally, was ordered to pay plaintiff's attorney fees totaling $1,408,877. (Ex. 2.)

After receiving the final judgments, Applicant and his co-defendants met with their counsel, continued to assert that they had done nothing wrong, and requested that their attorneys file an appeal. The attorneys filed an appeal of the decision to the state supreme court, which agreed to hear their appeal in April 2011. The attorneys representing Applicant and his co-defendants filed their opening brief in May 2011, and the opposing party filed its reply brief in July 2011. (Ex. 1-2, enclosure 2, enclosure 3. enclosure 4; Ex. 1-F; Ex. 1-G; Administrative Notice Document 4; Tr. 1:15, 73, 91-92.)

The appeal identifies five assignments of error. Two assignments of error cited abuse of discretion by the trial judge on the issue of opinion testimony by plaintiff's expert witness and failure to permit rebuttal testimony by the defendants' expert witness. One assignment of error challenged the trial court's failure to set aside damages based upon a specific model of goodwill damages; another assignment of error alleged trial court error in failing to set aside the jury verdict awarding duplicative trebled and punitive damages. The fifth assignment of error alleged that the trial court erred in failing to set aside damages that were costs of litigation. The defendants' liability under the state uniform trade secrets act and the state business conspiracy act was not challenged on appeal. (Government Administrative Notice Document 4.)

The state supreme court ruled in these matters on June 7, 2012. It held that Company A's evidence was insufficient, as a matter of law, to support an award of lost goodwill damages resulting from the conspiracy, and the trial court erred when it refused to set aside an award of damages relating to Company A's lost goodwill. The supreme court upheld the trial court's awards of trebled and punitive damages in favor of Company A. The supreme court also affirmed the trial court's awards to Company A for computer forensics damages and affirmed an award of $350,000 in punitive damages against each of the defendants on Company A's trade secrets claim. Because the computation of damages had been modified, the supreme court remanded the award of attorneys' fees relating to Company A's statutory business conspiracy claim. No modifications or changes were made to the trial court's findings of Applicant's liability. (Ex.2-8.)

Three of Applicant's co-defendants testified as witnesses at his DOHA hearings. One of the witnesses was the chief executive officer and president of the company where Applicant is now employed. The other witness is a vice president of the company and Applicant's supervisor. When discussing the civil judgment against them, one of the witnesses stated that he believed he had done nothing wrong. The other witness stated he did not know why Company A brought the lawsuit against him and the other co-defendants. The witness who was president of the company stated that Applicant was the assistant facility security officer at the company. The witnesses spoke highly of Applicant and stated that he was reliable and followed rules and regulations. (Tr. 1:116-150; Tr. 2: 211-212.)

Applicant also offered four letters of character reference. The authors of the letters were former colleagues and friends who had known Applicant for many years. These individuals praised Applicant's outstanding military record, strong work ethic, high moral character, reliability, and trustworthiness. (Ex. B; Ex. C; Ex. D; Ex. E.)

At his remand hearing, Applicant testified that he has thought about the issues related to his case every day for over three years. He stated that he was well-respected at Company A and always tried to be honest and above board. (Tr. 2: 94-96.)

Policies

The U.S. Supreme Court has recognized the substantial discretion of the Executive Branch in regulating access to information pertaining to national security, and it has emphasized that "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 an 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 and modified.

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 used 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, the administrative judge applies these guidelines in conjunction with the factors listed in the adjudicative process. 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.

Under Directive ¶ E3.1.14, the Government must present evidence to establish controverted facts alleged in the SOR. Under Directive ¶ E3.1.15, the Applicant is responsible for presenting "witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by applicant or proven by Department Counsel. . . ." The Applicant has the ultimate burden of persuasion in seeking to obtain a favorable security 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 E, Personal Conduct

AG ¶ 15 explains why personal conduct is a security concern:

> 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.

SOR ¶ 1.c. states that Applicant has filed an appeal of the civil judgments alleged in the SOR. Applicant admitted this allegation. However, the allegation, as framed, does not specify conduct that raises a security concern under Guideline E. Accordingly, I conclude SOR ¶ 1.c. for Applicant.

However, the remaining Guideline E allegations in the SOR do raise security concerns. As the former employee of two defense contractors (Company A and Company B) and the current employee of a third defense contractor, Applicant seeks a security clearance. In June 2010, after an 11-day civil trial, at which he was represented by counsel, testified, and was cross-examined, a jury found against Applicant on the following claims: breach of fiduciary duty; breach of contract; violation of a state computer crimes act; violation, in concert with other defendants, of a state business conspiracy act; civil conspiracy, in concert with other defendants; misappropriation of trade secrets; and conversion. The action was brought against Applicant by his former employer, Company A.

Applicant's personal conduct raises security concerns under Guideline E disqualifying conditions AG ¶¶ 16(c) and 16(d). AG ¶ 16(c) reads: "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 person may not properly safeguard protected information. AG ¶ 16(d) reads: "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 . . . (3) a pattern of dishonesty or rule violations."

Two Guideline E mitigating conditions might apply to the facts of this case. Applicant's disqualifying personal conduct might be mitigated under AG ¶ 17(c) if "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." AG ¶ 17(d) might apply if "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."

As a federal contractor and high-level manager and supervisor, Applicant was entrusted not only with classified and sensitive information, but also with Company A's trade secrets and proprietary information. Soon after he left Company A and went to work for Company B, Company A brought a civil action against Applicant and others alleging civil conspiracy, conversion, breaches of contract and fiduciary duty, as well as violations of his state's computer crimes act, business conspiracy act, and trade secrets act. A jury found Applicant liable for willful and malicious misappropriation of Company A's trade secrets. The presiding judge assessed him $350,000 in punitive damages. Along with three co-defendants and Company B, Applicant was assessed joint and several damages for violating his state's business conspiracy act. Additionally, he and his co-defendants and Company B were also ordered to pay plaintiff's attorney fees. Applicant insisted he "had done nothing wrong" at his January 2012 DOHA hearing and at his September 2012 remand hearing. However, in their appeal to the state supreme court, Applicant and his co-defendants did not contest their liability as found by the jury and confirmed by the judge in their civil trial.

Applicant's personal conduct, which involved failure to follow rules and regulations for safeguarding his employer's trusted information, was not minor, so remote in time, so infrequent, or occurred under such unique circumstances that it was unlikely to recur and therefore did not cast doubt on his reliability, trustworthiness, or good judgment. (AG 17(c).)

Applicant insisted he had done nothing wrong. The trial record contained e-mails that Applicant admitted he sent and received as he participated in efforts to recruit a group of Company A employees who would go to work for Company B. As Company B employees, they planned to compete for a contract they had worked on as employees of Company A. At his civil trial, Applicant admitted he attached a 100-gigabyte hard drive to his Company A computer and copied hundreds of company files to that external drive. He then deleted hundreds of files from his computer and from his computer's recycle bin. He claimed he left the 100-gigabyte hard drive at Company A when he left so that his successor, his deputy, could use the company information to carry out his duties. Nothing in the record substantiated his claim. When he copied the company files on June 2, 2009, Applicant had reason to know that his deputy had given notice to Company A at the end of May and had, like Applicant, accepted employment with Company B. Moreover, the deputy testified that he had all the information he would have needed to carry out his increased responsibilities on his own Company A

computer, and he had no need of the information Applicant had copied to the 100-gigabyte hard drive. He also stated he never received the 100-gigabyte hard drive.

Applicant was unable to account for the whereabouts of the 100-gigabyte hard drive. He did not identify it or turn it over to Company A at his exit interview. None of the files he copied appeared on his Company B computer.

Applicant failed to demonstrate that he understood the gravity of the conduct for which the jury found him responsible. He repeatedly insisted he had done nothing wrong, and he failed to demonstrate that he understood what had caused his unreliable conduct. He was unable to ensure that such behavior was unlikely to recur. (AG ¶ 17(d).) I conclude, therefore, that neither of the applicable personal conduct mitigating conditions applies to the facts of Applicant's case.

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 relevant 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.

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 has a distinguished military record, and he is considered to be a valued employee by his current and former colleagues. However, Applicant failed to mitigate security concerns arising from his personal conduct as a defense contractor. His former employer, Company A, made several serious allegations against Applicant. Those charges were adjudicated in an 11-day civil jury trial. Applicant was represented by counsel; he testified and was cross-examined. After the jury returned a verdict against Applicant and his co-defendants, the presiding judge reviewed the record, affirmed the jury's findings of liability, and entered final judgments specifying money damages. While Applicant denied any wrongdoing, he failed to rebut or mitigate the allegations, which raised security concerns about his reliability, trustworthiness, and ability to follow rules.

Applicant joined with others to misappropriate his employer's proprietary and trade secret information. He participated in activities to encourage other employees of Company A to accept employment with Company B.

Applicant's reason for copying hundreds of files containing proprietary and trade secret information from his Company A computer to a 100-gigabyte hard drive was not credible. He said he copied the files on June 2, 2009, to the 100-gigabyte hard drive to give to his deputy so that he could carry out Applicant's duties at Company A after Applicant left to work at Company B. However, Applicant had good reason to know that his deputy had resigned from Company A at the end of May 2009 to join him as an employee of Company B. Further, his inability to account for the 100-gigabyte external drive raises serious concerns about his truthfulness, reliability and judgment.

After a thorough review of the evidence in the record of this case, and after carefully observing Applicant and assessing his demeanor and credibility, I conclude that Applicant failed to mitigate the security concerns arising under the personal conduct adjudicative guideline.

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 E:	AGAINST APPLICANT
Subparagraphs 1.a(1) - 1.a(7):	Against Applicant
Subparagraphs 1.b(1) - 1.b(3):	Against Applicant
Subparagraph 1.c:	For Applicant
Paragraph 2, Guideline F:	FOR APPLICANT
Subparagraph 2.a.:	For Applicant[7]

[7] Although the Guideline F allegation was concluded for Applicant in the March 8, 2012, decision and was not appealed, I include it in the Formal Findings in this case to complete the record.

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.

_____

Joan Caton Anthony
Administrative Judge