DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 11-02724
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Braden M. Murphy, Esquire, Department Counsel
For Applicant: Holly Svetz, Esquire and Steven Cave, Esquire

02/28/2013

Decision

CREAN, Thomas M., Administrative Judge:

Based on a review of the pleadings, exhibits, and testimony, eligibility for access to classified information is granted.

Statement of the Case

Applicant had been granted eligibility for access to classified information in 2001. On June 6, 2010, Applicant submitted an Electronic Questionnaire for Investigations Processing (e-QIP) to continue a security clearance required for a position with a defense contractor. The Department of Defense (DOD) issued interrogatories to Applicant to clarify or augment potentially disqualifying information. After reviewing Applicant's response to the interrogatories, DOD could not find that it is clearly consistent with the national interest to continue his security clearance. On July 25, 2012, DOHA issued a Statement of Reasons (SOR) detailing security concerns for personal conduct under Guideline E. This 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 in the DOD on September 1, 2006. Applicant acknowledged receipt of the SOR on August 1, 2012.

The Government alleges two security concerns under Guideline E. Applicant answered the SOR through counsel on September 13, 2012. He provided an eight-page response and two extensive exhibits. Applicant denied the first security concern (SOR 1.a). He admitted in part and denied in part the second security concern (SOR 1.b). He requested a hearing before an administrative judge. Department Counsel was prepared to proceed on October 11, 2012. The case was assigned to me on October 22, 2012. The Defense Office of Hearings and Appeals (DOHA) issued a Notice of Hearing on November 9, 2012, for a hearing on December 4, 2012. I convened the hearing as scheduled. Two witnesses testified for the Government. The Government offered 11 exhibits, which I marked and admitted into the record as Government exhibits (Gov. Ex.) 1 through 11.[1] Applicant and two witnesses testified. Applicant offered two exhibits which I marked and admitted into the record without objection as Applicant Exhibits (App. Ex.) A and B. DOHA received the transcript of the hearing (Tr.) on December 13, 2012.

Procedural Issues

On October 24, 2012, Applicant moved to have his case heard by another administrative law judge who had heard and decided a companion case. On November 1, 2012, Department Counsel filed a brief opposing the transfer. Since good cause was not shown why the case should be transferred, I denied the request on November 6, 2012. (Tr. 12; *See*, Hearing Exhibit I)

Findings of Fact

After a thorough review of the pleadings, transcript, and exhibits, I make the following essential findings of fact. Applicant admitted one and denied in part the other allegation of misconduct under personal conduct. His admission is included in my findings of fact.

Applicant is 38 years old and employed as a systems engineer for a defense contractor. He graduated from high school in 1993, and has approximately three years of college. In college, he worked part-time for the college in their computer operations. Instead of completing college, he went to work in the computer technology field. He worked for various companies, including defense contractors, before starting work for his present employer in 2008. He was first granted access to classified information in 2001. He is married with two children. (Tr. 167-170; Gov. Ex. 1, e-QIP, dated June 1, 2010)

[1] Applicant did not object to Exhibits 1, 2, and 4 to 11. He did object to parts of Gov. Ex. 3. Gov. Ex. 3 was the transcript of a deposition Applicant gave in a federal court case. Applicant authenticated the transcript as accurate in Gov. Ex. 4. The objection was overruled and the document was admitted. (Tr. 37-42)

Applicant started working for Dr. L, his mentor, at a defense contractor in approximately 2005. When Dr. L left to work for company R in 2006, Applicant followed him to company R in August 2006 as a consultant on classified projects in a DOD data center. He worked on business development and proposals as well as being the enterprise storage architect for a large defense program. In August 2007, the security clearance of company R's president, Mr. N, was revoked, making the facility security clearance of the company defective. A new organization had to be established for company R to continue to work on classified contracts. As the leader of the government contracting unit of company R, Dr. L proposed a novation plan to Mr. N to transfer the classified contracts to a company that he formed years earlier, Q3, but never implemented. The Government had to approve any plans so the new organization could continue to work on the classified contracts previously awarded to company R. Applicant participated in a few meetings and discussions during March and April 2008 on the transfer of the classified contracts to a new company, so that he was aware of the potential novation of contracts to Q3. The contracts had not been transferred to a new contractor by May 2008. The indications were that Mr. N was reluctant to make changes because he could possibly lose his share of profits from the contracts. There were ongoing discussion between Mr. N, the attorneys for company R, Dr. L, and possibly the Government contracting officer's representative. There were major disagreements between Mr. N and Dr. L on the plans and implementation.

Mr. N terminated Dr. L's employment with company R on May 1, 2008. Dr. L left company R that day. He then incorporated a new company QB in May 2008. In June 2008, Mr. N and company R sued Dr. L, Applicant, and three other individuals who went to work at QB, in federal court for breach of their employment contracts and breach of trust and loyalty to company R. After depositions were taken from some of the individuals involved in company R and QB, the court action was settled and dismissed. (*See,* Gov. Ex. 3, Deposition transcript at 10-34; Tr. 133-145; Gov. Ex. 11, resume, undated; App. Ex. B, e-mails, date April 29, 2008)[2]

The SOR alleges that Applicant breached his loyalty to company R in May 2008 by planning with others to start a competing business (SOR 1.a). He denied this allegation. The SOR also alleges that after resigning from company R in May 2008, he improperly and without authorization deleted company R files and business records from his company R computer and copied the records onto his own computer. Applicant admitted that he deleted the files after copying them to his own personal computer. He denied that he deleted the files with the deliberate intent to harm the business interests of company R. The Government's allegation is basically that he breached his loyalty to his former employer and then tried to cover-up his actions. (Tr. 16-19; *See,* Response to SOR, dated September 13, 2012)

On May 19, 2008, Applicant notified company R that he would leave company R at the end of May 2008. Dr. L's departure did not affect the work Applicant was doing for company R, but he knew Dr. L intended to start a new company to pursue business. In early May 2008, he discussed salary and employment opportunities with Dr. L about

[2] The parties agreed to stipulate to these facts. (Tr. 16)

working at the new company. Applicant wanted to move with Dr. L because he worked for him for a number of years and they were always working on "cool" technology projects. In addition, the work he was doing with company R was becoming more mundane and operational rather than developmental. He was concerned about the future of company R because of the failure to reach agreement on a novation plan, the potential end of funding on the contracts, and the lack of vision for company R caused by the departure of Dr. L. Applicant did not know if he had a valid future with company R, so he took a leap of faith and went to work with Dr. L in his new company. The company had no business and no income, just employees. He wanted to follow Dr. L because he thought Dr. L provided the direction while he was the core capability for company R. He did not leave believing the new company was formed to compete with company R. By May 19, 2008, Dr. L had recruited two or three employees of company R, including Applicant, to work for him in QB. Applicant never discussed or tried to market any work he was doing with company R with any employee of QB. (Tr. 167-183)

The Government's information on the security concern raised in SOR 1.a is based on responses Applicant gave to questions asked at a deposition in the federal court action. He testified in the deposition and at the hearing that in May 2008, he decided to leave company R, after Dr. L was terminated, and move with him to his new company, QB. Shortly after he agreed to move to QB and had notified company R that he was leaving, using his wife's private e-mail account, Applicant sent information to Dr. L of potential contracts for the new company. The information he provided was based on proposals he created at the request of the Government contracting officer for the data center while working for company R. The information centered on projects under discussion for the data center. He knew of the projects since he worked on project planning as an employee of company R. As part of his work, he actually developed the plans for the Government. The information was about potential future work that may be needed in the data center. The projects were not funded and were basically items that could potentially be requested and funded. He developed a bill of materials for the projects that could be provided by a contractor. In developing the list, his aim was to include as many items as possible that may be needed by the data center. The information contained his best guess on the proposed budget and cost of items to be used by the Government for planning purposes only.

Applicant used his wife's computer account because he did not have a personal e-mail account, and he wanted to separate the information he forwarded from his work at company R. He did not consider the information he sent Dr. L to be business information since it did not have funding or a contract associated with it. He considered the information public since it was available to and known by most if not all of the contractors that were working in and on data center projects. He did not believe company R or any of its subsidiaries could perform the work because the company no longer had a facility security clearance for classified work. He knew that any company could make a proposal for work on unfunded requirements. However, there had to be funding and a contract before work could be awarded. Companies would have to bid on the work and actual cost would be determined if a contract was awarded.

Applicant forwarded the information because he did not know if Dr. L was aware of the potential work even though the list was developed prior to Dr. L being terminated by company R. He did not know if Dr. L had seen the list of potential work. He was unsure of the business potential of the new company or what Dr. L intended for the company to pursue. He considered the information to be public and available to all potential contractors. (Tr. 184-186, 195-203; Gov. Ex.3, Deposition, dated September 2, 2008, at 78-95)

When Applicant started working for company R, he was provided a company laptop computer to use in his business activities. Company R had no policy concerning what information could be placed on the company laptops. There also was no policy concerning the information and material an employee could take when leaving the company. If there was any such policy, Applicant had never been advised or trained in the policy. Applicant stored his personal information, including bank account information, music files, and other private information on his company-R-issued laptop. When he notified company R that he was leaving their employment, arrangements were made for him to turn in his security passes, company-provided cellphone, laptop, and other equipment. Applicant worked at a site different from the company headquarters. On his last day with company R, May 30, 2008, Applicant returned his security passes to a Government representative. He left his company-ssued cellphone and other equipment with a company representative. Since he worked at a secured facility and was unable to take his unsecured company-issued laptop into the facility, he did not have the laptop with him. He made arrangements with a representative of company R to return the laptop to him in a parking lot where he worked on June 10, 2008. (Tr. 45-75, 186-210)

A forensic computer expert examined the laptop computer for company R to determine if there were files on the computer that were the property of company R, how the computer may have been used, and if the use violated any law or policy of company R. He did not receive policy information on use of company computers from company R. The expert testified that he performed a preliminary examination of the laptop's programs and stored files. He discovered that there was little data on the computer that would enable him to draw significant conclusions about how the computer was normally used. It appeared that a good deal of the information that would have been contained in the standard locations had been deleted. There was evidence that some files had been contained on the system but were now deleted. He identified the files as not being related to company R but to another business, Q3. (Tr. 75-79)

The expert noted that a legally available utility, called Sdelete, had been run on the system. This program would not be known to a typical computer user, but would be used by a sophisticated knowledgeable computer savvy person. The utility is used as an anti-forensic tool to make files that may have been deleted permanently unrecoverable. It finds the space where the file had been located and overwrites it with random data, so that the original file can no longer be retrieved. The program as used on this computer was targeted to specific files and was not a blanket deletion of the data on the computer. It deletes the data but still indicates the file existed on the master list.

The deletion was done in a way that would leave the system intact and still functional. It targeted the files the person running Sdelete wanted deleted. The event log contained only one day of data where normally such a file contained weeks and even months of data. The data was only for dates between June 9 and June 10, 2008.

There was evidence that external storage devices had been attached to the computer usually for the purpose of copying files to an external device. There was no evidence that company R files had been on the computer. However, there is an indication that a file pertaining to the budget for Q3 had been received from an external source and stored on the laptop by Applicant. The expert concluded that prior to the computer being returned to company R, a significant effort by a reasonably sophisticated user erased much of the content of the computer, as well as any indications of the user's actual use of the computer. (Tr. 79-81)

The expert also noted that there are circumstances where overwriting used files with random data is appropriate to protect private information. He would advise that if a computer was to be donated, all personal data be removed so it could not be retrieved. However if the computer was to be returned to an employer, this would not be the typical mechanism used to delete files. It may delete vital information of the business. When the computer is the property of a business and not an individual, it was his opinion that this was not the common technique used to delete data. The data regarding the activities of the user would be deleted by Sdelete. Using some sort of file-wiping system would not be unusual. But only someone with sophisticated knowledge of programs and computers would use something like Sdelete. It would delete not only personal information and music files but other files of interest to the business. He was able to determine that Applicant was the primary user of the laptop. He found traces of some, but not all, files Applicant had on the computer. The external devices could have been used to save files and presentations. There was no indication that any deleted files may be available to company R from other sources or on the company's master files. There was no indication that any files were copied or transferred for unauthorized purposes. (Tr. 81-121)

Applicant was not aware of any company policy concerning deletion of information and he had not received any training on any such action. Before returning his company R computer, he wanted to be sure all of his personal information and files were deleted. In previous positions working on Government computers, personal profiles and information were deleted before reissuing the computers. The data deletion was performed to ensure there was no accidental spillage of classified information or personal information. In his past positions, he took a broad range of actions to delete information from computer files before reissuing a computer to another person. On June 9, 2008, Applicant copied his personal information on the company R laptop computer to his new computer by copying the entire directory of files rather than copying files individually. He deleted his personal information files, including his financial information, and music files from the computer. He also deleted some data and e-mails he received concerning Q3. His intent was to restructure the data, and delete any information he did not need in his new position. A list of file names would still be available but not data

within the files. He ran the Sdelete program to be sure that all his personal data was deleted from the computer. He also deleted Q3 reference data since he did not believe the material was his or company R property, and he did not have authorization to provide the data to company R.

Applicant acknowledged that he returned his company R laptop computer to a company representative on June 10, 2008. He was not concerned with potentially deleting company R material because he knew the material was stored on a company computer storage site. He did not intend to delete any company R or Government deliverable material. He wanted to leave the laptop operable so company R could log in and retrieve company R or Government deliverable material. Some company R material was transferred when he copied files to his new computer. He intended to delete the information from his new computer but did not have a chance before litigation started. He used Sdelete in the past because it is a free program used by other government agencies to overwrite data. (Tr. 145-195, 203-208)

Applicant believed the duty he owed company R when he resigned was to continue to support the contracts he was assigned until his resignation was effective. He continued to work on business development activities until he left. He also has a duty to safeguard company R information. He had a duty to return his laptop in a state that company R could still use it to access its information. He wanted to leave the company in a favorable friendly manner. There was no evidence that he had a do-not-compete agreement with company R. He was not an executive of the company but a low-level worker and project manager. (Tr. 210-222)

His discussions with Dr. L about the new company centered more on his salary and position than potential business opportunities. They did not talk in detail about contracts that company R could still compete on and manage. Dr. L had more information on company R than he did. Dr. L knew in detail all of the opportunities being worked by company R. (Tr. 208-210)

A senior executive and part-owner of Applicant's present employer testified that he has known Applicant for almost ten years. He first knew Applicant when they both worked for different companies supporting the same government agency. He not only sees Applicant at work but their families also socialize together. He considers Applicant to be honest, reliable, and with the highest integrity. He has complete trust in Applicant and feels he should receive access to classified information. (Tr. 124-132)

Dr. L testified that he has known Applicant for approximately ten years. He recruited Applicant to fill a challenging technical strategic role for the witness's defense-contractor employer. Applicant had technical expertise, business intelligence, and understood organizational needs. When Dr. L moved to company R, he hired Applicant to work in a strategic position for company R. Applicant was instrumental in developing solutions for company R projects since Applicant is very determined to solve problems. He learns all aspect of the problem and understands the business practices, policies, and technical issues. Dr. L socializes with Applicant and his family. Applicant has

always shown good responsible business judgment. He is worthy of a position of trust and access to classified information. (Tr. 148-156)

Policy

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 must be considered 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. 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, 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 for obtaining 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 protect classified information. Such decisions entail a certain degree of legally permissible extrapolation about potential, rather than actual, risk of compromise of classified information.

Analysis

Personal Conduct

A security concern is raised because conduct involving questionable judgment, untrustworthiness, unreliability, or unwillingness to comply with rules and regulations can raise questions about an individual's reliability, trustworthiness, and ability to protect classified information. Personal conduct is always a security concern because it asks the central question does the person's past conduct justify confidence the person can be entrusted to properly safeguard classified information. (AG ¶ 15)

The Government allegation is that Applicant breached his duty of loyalty to company R by planning with others to start a competing business. The Government information on this allegation was from a deposition taken from Applicant. In the deposition, Applicant admitted he agreed to join the new company and communicated potential work project information to the founder of the new company. Applicant knew about the potential projects from his work as an employee of company R. Applicant admitted he deleted certain information from his company R computer before returning it. This information is sufficient to raise Personal Conduct Disqualifying Conditions AG ¶ 16(c) (credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any other single guideline, but which, when considered as a whole, supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the person may not properly safeguard protected information); and AG ¶ 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).

The Government produced sufficient evidence to establish the disqualifying conditions as required in AG ¶¶ 16(c), and 16(d). The burden shifted to Applicant to produce evidence to rebut, explain, extenuate, or mitigate the security concerns under personal conduct. An applicant has the burden to prove a mitigating condition, and the burden to prove or disprove it never shifts to the Government.

Applicant presented information to explain, rebut, and extenuate the security concerns raised by the Government. I considered this information in regard to Personal Conduct Mitigating Conditions AG ¶ 17(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 is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment); and AG ¶ 17(f) (the information was unsubstantiated or from a source of questionable reliability).

When Applicant's mentor and friend, Dr. L, was terminated by their mutual defense contractor employer and formed a new company, Applicant agreed to work for the new company. There was no evidence presented that Applicant had a do-not-compete agreement with company R. Since Applicant and Dr. L were computer technology experts and worked in that field for company R, the new company would be working in the computer technology field. The new company would undoubtedly be competing with company R for future government contracts. Applicant had a reasonable basis to leave company R and work for QB. He no longer enjoyed the work he was doing at company R and he was concerned for the company's future. He enjoyed working for Dr. L and considered him a friend and mentor. After notifying company R that he was leaving for the new company, Applicant sent information to Dr. L on potential business opportunities for the new company. He learned of these opportunities when as an employee of company R, he developed the information for the Government contracting officer. The information was not company R proprietary information but common information on future potential business opportunities. The information was known and available to all potential contractors. It was only potential work that the Government may in the future request. The potential projects were not funded and there were no contracts provided by the Government. Applicant's actions in joining the new company and sending common information to his new employer did not undermine or affect the possible business potential of company R. The company did not lose any contracts or work based on Applicant's action and it still had the ability to compete as a contractor for the same work that QB would be competing for.

The information presented by Applicant refuted and mitigated the security concern raised by the Government's information. He had reasonable, plausible, and credible reasons for his actions. He had good and valid reasons for leaving company R and moving to another company. There was no prohibition against him going to work for the new company. He was a low-level employee of company R and he did not have a do-not-compete agreement. He forwarded to his future employer common information available to any company. The projects had not been funded or placed for contract. The information was merely speculative as to potential future work. The Government still had to fund the work and contractors had to win a contract to do the work. It was not proprietary business information that was damaging to company R's business. The transmission of this information under the circumstances did not rise to the level of a security concern. The situation was unique and does not cast doubt on his reliability, trustworthiness, and good judgment.

Applicant admitted that he used a computer program to delete information from his company R computer before returning it. He presented reasonable, logical, and credible explanations for his action in deleting information from the laptop computer. Applicant is a computer expert who in the past had worked on computers being returned and recycled. He had personal information on the computer and wanted to delete the personal information since he did not know how and by whom the computer would be used in the future. He was familiar with a sophisticated program that would overwrite and delete the data from his accounts but still have the computer available to this former employer for their use. He ran that program with the intent that the computer could be

used again. Since Applicant had reasonable bases for all of his actions, he refuted and mitigated the personal conduct security concerns under Guideline E.

Whole-Person Analysis

Under the whole-person concept, the administrative judge must evaluate an applicant's security eligibility by considering the totality of the applicant's conduct and all the circumstances. An 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 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. I considered the information provided by his supervisors concerning his reputation for honesty, reliability, and trustworthiness. I considered that Applicant has been eligible for access to classified information for many years without incident. Applicant's actions in sending information to his future employer and deleting files from his computer were not inappropriate and illogical. He sent his future employer only information that was commonly available to all potential contractors. He deleted his communications with his future employer from his computer while erasing his personal files and data from his computer before returning it. He has appropriate reasons for his actions so that the actions do not cast doubt on his reliability, trustworthiness, and ability to protect classified information. How he handled his departure from company R, his new employment with QB, and the return of his computer to company R indicate he would properly handle, manage, and safeguard classified information. The record evidence leaves me without questions and doubts about Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude Applicant has mitigated the personal conduct security concerns.

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:	FOR APPLICANT
Subparagraphs 1.a - 1.b:	For Applicant

Conclusion

In light of all of the circumstances presented by the record in this case, it is clearly consistent with the national interest to grant Applicant eligibility for a security clearance. Eligibility for access to classified information is granted.

_____
THOMAS M. CREAN
Administrative Judge