DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
----------	)	ISCR Case No. 18-00554
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government:
Jeff Nagel, Esquire, Department Counsel[1]
Tara Karoian, Esquire, Department Counsel[2]

For Applicant:
Pro se

July 17, 2019

_____

Decision

_____

ROSS, Wilford H., Administrative Judge:

Statement of the Case

Applicant submitted his Electronic Questionnaire for Investigations Processing (e-QIP) on April 22, 2017. (Government Exhibit 1.) On March 12, 2018, the Department of Defense Consolidated Adjudications Facility (DoD CAF) issued a Statement of Reasons (SOR) to Applicant, detailing security concerns under Guideline M (Use of Information Technology), and Guideline E (Personal Conduct). The action was taken under Executive Order 10865, *Safeguarding Classified Information Within Industry* (February 20, 1960),

[1] Mr. Nagel appeared at the August 21, 2018 hearing only.
[2] Ms. Karoian appeared at the September 19, 2018 hearing only.

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 effective within the Department of Defense after June 8, 2017.

Applicant answered the SOR in writing (Answer) on March 30, 2018, with attachments, and requested a hearing before an administrative judge. Department Counsel was prepared to proceed on June 27, 2018. The case was assigned to me on July 11, 2018. The Defense Office of Hearings and Appeals (DOHA) issued a Notice of Hearing on July 18, 2018. The hearing was conducted on August 21, 2018, and September 19, 2018.

The Government offered Government Exhibits 1 through 3, which were admitted without objection. Applicant offered Applicant Exhibits A through H, which were admitted without objection, and testified on his own behalf. The record remained open for the receipt of additional documentation. DOHA received the final transcript of this hearing on September 27, 2018. Applicant submitted an additional statement with his comments concerning the transcript on October 2, 2018. That document is marked and admitted as Applicant Exhibit I. The record then closed.

Findings of Fact

Applicant is 51 years old and is being sponsored for a security clearance by a defense contractor. He is married and has a doctorate degree. Applicant owns his own company, but used to be employed by Company A.

Paragraph 1 (Guideline M, Use of Information Technology)

The Government alleges in this paragraph that Applicant is ineligible for national security eligibility and a security clearance because he failed to comply with rules, procedures, guidelines, or regulations pertaining to information technology systems.

Paragraph 2 (Guideline E, Personal Conduct)

The Government alleges in this paragraph that Applicant is ineligible for national security eligibility and a security clearance because he engaged in conduct that involved questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations, thereby raising questions about his reliability, trustworthiness, and ability to protect classified or sensitive information.

Both allegations in this case refer to a single act by Applicant in the days before he was terminated from his employment with Company A. Applicant was hired by Company A in June 2009 to fill a senior management position related to his particular area of expertise. He is an acknowledged expert in his field, which is limited to a very

small number of people and companies. Company A expected Applicant to help grow their business in this field, which he did for several years. (Tr. 27-28.)

Beginning in 2014, the relationship between Applicant and the leadership of Company A began to sour. Applicant approached the Chief Executive Officer (CEO) of Company A and alleged that another senior manager was actively defrauding the Federal government. The CEO said that he would look into it but, according to Applicant, instead the CEO set about making Applicant's continued employment at Company A untenable. (Answer; Applicant Exhibit F; Tr. 28, 75-76.)

The situation came to a head in early June 2015. On June 3, 2015, a coworker and friend of Applicant, Mr. E, was let go by Company A. Whether Mr. E actively resigned, his threat to resign was accepted, or he was terminated, is of little significance to the Applicant's national security eligibility. In any event, Mr. E's departure convinced Applicant he could no longer work for Company A. (Answer; Applicant Exhibits A and F; Tr. 82-84.)

On June 4, 2015, before normal work hours, Applicant arrived at his office. According to Applicant he often did this. That morning Applicant printed out a copy of his Outlook contacts from Company A's computer system. Included in the Outlook file were contacts that Applicant had before his employment, as well as those he acquired after he began employment, which included employees of Company A. Applicant stated that he printed out the Outlook file so that he could go through it and separate out those contacts that he had prior to employment with Company A, which the company had wanted him to do for some time. (Applicant Exhibit F at Attachment 2; Tr. 59-61, 71-74.)

Applicant stated that later in the morning of June 4, 2015, he had a discussion with the CEO, during which Applicant berated the CEO for Company A's conduct towards Mr. E, and informed the CEO that he wished to leave his employment with Company A in the near future. He then left his place of employment with a folder containing the Outlook printout. At this point, it is important to note, all parties agree that Applicant had not resigned or been terminated. (Answer; Government Exhibit 2; Applicant Exhibit F at Attachment 5; Tr. 28-29, 61-63, 75, 85-86.)

Company A wrote the Office of Personnel Management a letter dated May 25, 2017, which concerned Applicant's conduct. That letter stated:

> On June 4, 2015 [Company A's] Information Technology Department (IT) observed [Applicant] accessing and printing out [Company A's] proprietary customer data as well as [Company A] contact information. There was no legitimate business reason for this action and it occurred early in the morning (between 6:47 am and 6:50 am) when, by [Applicant's] own words, he was "not on the clock." (Government Exhibit 3 at 1.)

Based on the above-described conduct, according to Company A, the decision was made to terminate Applicant for cause for violating the terms of his employment contract. Applicant was informed of this fact in an email dated June 6, 2015. There is no allegation or evidence that Applicant took any other type of proprietary information. (Government Exhibit 3; Applicant Exhibit F at Attachment 5.)

Company A subsequently sent a letter to Applicant dated June 11, 2015. In that letter Company A advised Applicant that they believed his conduct in printing the Outlook contacts file violated his employment agreement. In addition, and more pertinent to this decision, Company A felt that Applicant's conduct violated their "Proprietary Information and Assignment of Inventions Agreement" (PIAIA). (Government Exhibit 3.)

The PIAIA states in pertinent part that Applicant agrees:

> 1.1. Recognition of Company's Rights: Nondisclosure. At all times during my employment and thereafter I will hold in strictest confidence and will not disclose, use . . . any of the Company's . . . Proprietary Information . . . , except as such disclosure, use . . . may be required in connection with my work for the Company. . .
>
> 1.2. Proprietary Information. The term "Proprietary Information" shall mean any and all confidential and/or proprietary knowledge, data, or information of the Company. . . By way of illustration but not limitation, "Proprietary Information" includes . . . (b) customer/prospective customer information, customer/client lists and all lists or other compilations containing client, customer or vendor information. . . Notwithstanding the foregoing, it is understood that, at all such times, I am free to use information which is or becomes publicly known through lawful means, which was rightfully in my possession or part of my general knowledge prior to my employment with the Company as specifically identified and disclosed by me in Exhibit A-2, or which is disclosed to me without confidence or proprietary restriction by a third party who rightfully possesses the information (without confidential or proprietary restriction) and who did not learn of it directly from the Company. (Government Exhibit 3.)

Applicant argued that Company A's statement that he stole proprietary information in printing up the Outlook contacts list was a determination made after the fact to justify his termination. According to Applicant, Company A used his action as a subterfuge in order not to pay a substantial amount of money upon his leaving the company. He maintained that his conduct was appropriate, innocuous and within the scope of his employment at the time. He admitted that he wanted to separate out his contacts from the company's because he knew he was going to leave the company soon, not because he thought he would be terminated. Applicant did not believe that the Outlook contacts list was proprietary data. At that time Applicant also had a cell phone provided by

Company A that also contained the same Outlook contacts file. (Tr. 32-33, 57-58, 68-69, 71-74, 84-87.)

Within a week or so after leaving employment Applicant returned the Outlook contacts list to Company A's representative. (Answer at Exhibit 7 of Attachment 1; Applicant Exhibit F at Attachment 9; Tr. 67.)

Applicant soon became involved in litigation with Company A over his termination. That litigation was extensive and acrimonious. It eventually lead to an agreement between the parties in which Applicant received a monetary settlement. Applicant maintained that this litigation, along with other actions by Company A, were designed to prevent Applicant from working in the defense industry. Applicant submitted documents, pleadings and transcripts concerning this litigation. The statements made in these documents are given appropriate weight in this decision. (Answer at Attachments 1, 2, 3, 4, 5, 6, 7, 8, and 9; Applicant Exhibits A, B, D, E, and F at Attachments 1, 7, and 8; Tr. 29-30.)

Mitigation

Applicant was a valued member of Company A until the time of his termination, as shown by his performance appraisal dated October 2014. (Answer at Exhibit 3 of Attachment 1.)

Applicant provided letters of recommendation from people who know him in the defense industry. He is described as a man of character, a person who is trustworthy, and a valued professional. They all recommend him for a position of trust. (Applicant Exhibits C, G, and H.)

Policies

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

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 AG ¶ 2 describing the adjudicative process. The administrative judge's overarching adjudicative goal is a fair, impartial, and commonsense decision. The entire process is a conscientious scrutiny of applicable guidelines in the context 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, "Any doubt concerning personnel being considered for national security eligibility will be resolved in favor of the 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. I have not drawn inferences based on mere speculation or conjecture.

Directive ¶ E3.1.14, requires the Government to 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 the applicant or proven by Department Counsel, and has the ultimate burden of persuasion as to obtaining a favorable clearance decision."

A person who seeks access to classified information enters into a fiduciary relationship with the Government predicated upon trust and confidence. This relationship transcends normal duty hours and endures throughout off-duty hours. The Government reposes a high degree of trust and confidence in individuals to whom it grants national security eligibility. 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 or sensitive information. Finally, as emphasized in Section 7 of Executive Order 10865, "Any determination under this order adverse to an applicant shall be a determination in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." *See also* Executive Order 12968, Section 3.1(b) (listing multiple prerequisites for access to classified or sensitive information.)

Analysis

Paragraph 1 (Guideline M, Use of Information Technology)

The security concerns relating to the guideline for use of information technology are set out in AG ¶ 39, which states:

> Failure to comply with rules, procedures, guidelines, or regulations pertaining to information technology systems may raise security concerns about an individual's reliability and trustworthiness, calling into question the willingness or ability to properly protect sensitive systems, networks, and information. Technology includes any computer-based, mobile, or wireless device used to create, store, access, process, manipulate, protect, or move information. This includes any component, whether integrated into a larger system or not, such as hardware, software, or firmware, used to enable or facilitate those operations.

AG ¶ 40 describes two conditions that could raise security concerns and may be disqualifying in this case:

> (d) downloading, storing, or transmitting classified, sensitive, proprietary, or other protected information on or to any unauthorized information technology systems;
>
> (e) unauthorized use of any information technology system; and
>
> (f) introduction, removal, or duplication of hardware, firmware, or media to or from any information technology system when prohibited by rules, procedures, guidelines, or regulations or when otherwise not authorized.

AG ¶ 41 describes one condition that could mitigate the above security concerns:

> (a) so much time has elapsed since the behavior happened, or it happened under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment; and
>
> (b) the misuse was minor and done solely in the interest of organizational efficiency and effectiveness.

Applicant left Company A under very contentious circumstances about which there continues to be factual disputes, as set forth in the record. In preparation for leaving the company, but while still employed, Applicant printed up his Outlook contacts file on June 4, 2015. This turned out to be Applicant's last day of work. Company A stated that Applicant's conduct in printing up the list amounted to theft of proprietary data, and that they fired him because of that act. Applicant stated that his conduct was allowable, certainly innocuous, and the list was not proprietary data. In analyzing this case two questions must be answered. Was the Outlook contact list proprietary data of Company A? If so, did Applicant's conduct amount to stealing it, or otherwise misusing it, in contravention of Company A's policies and procedures?

Applicant admits that his Outlook contacts list contained contact information that was obtained by him after he began working at Company A. Accordingly, it would come under the PIAIA ¶1.2. (b) "customer/prospective customer information, customer/client lists and all lists or other compilations containing client, customer or vendor information." However, it is also arguable that Applicant's Outlook contact list contained information obtained by Applicant that was viewed as an allowable exception to that rule. This is particularly true of information that can be obtained easily from other sources, particularly phone numbers and email addresses. (See *Centennial Bank v. Servisfirst Bank Inc.*, No. 8:16-cv-88-T-36JSS, 2016 WL 7325545, 7-8 (M.D. Fl. May 17, 2016) (Mag.), *adopted* 2016 WL 4238766 (M.D. Fl. Aug. 11, 2016.))

I find by substantial evidence that Applicant knew, or should have known, that the Outlook contact list contained at least some proprietary information belonging to Company A. Support for this finding is found in Applicant's statement that he was going to use the list to separate out the contacts that he had obtained before his employment with Company A from those he only knew about after his employment. Applicant admitted at the hearing that this fact was true.

Having determined that Applicant had downloaded proprietary information, we turn to the question of whether he stole it. Here, I find that there is insufficient evidence of such conduct. Applicant has never denied taking the list, did not destroy the list, and promptly returned it to Company A upon demand. The list may not be innocuous, but it is a stretch to call it important proprietary information.

Applicant maintained that Company A and its executives used this innocent incident as a subterfuge in order to terminate him for cause. He argues they did this so that they did not have to give him the multi-million dollar severance pay he would have been owed if he left the company under favorable circumstances. Based on other findings in this Decision, there is no need to make a finding as to the reasons for the conduct of Company A or its officers, and I am specifically not making any such finding.

Even assuming, for the sake of argument, that Applicant did take the list without authority, three years had passed since the incident as of the time the record closed. In addition, it occurred during a very strenuous and emotional time. Applicant was leaving a job he had worked at very successfully for several years. His outstanding job performance is shown by the 2014 evaluation contained in the record. Similar conduct is unlikely to recur, and it does not cast doubt on Applicant's current reliability, trustworthiness or good judgment. Guideline M is found for Applicant.

Paragraph 2 (Guideline E, Personal Conduct)

The security concerns relating to the guideline for personal conduct are set out in AG ¶ 15, which states in pertinent part:

> Conduct involving questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations can raise questions about an individual's reliability, trustworthiness, and ability to protect classified or sensitive information.

AG ¶ 16 describes two conditions that could raise security concerns and may be disqualifying in this case:

> (d) credible adverse information that is not explicitly covered under any other guideline and may not be sufficient by itself for an adverse determination, but which, when combined with all available information,

supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the individual may not properly safeguard classified or sensitive information. That 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 government protected information; and

(f) violation of a written or recorded commitment made by the individual to the employer as a condition of employment.

AG ¶ 17 describes one condition that could mitigate security concerns in this case:

(c) the offense is so minor, or so much time has passed, or the behavior is so infrequent, or it happened under such unique circumstances that it is unlikely to recur and does not case doubt on the individual's reliability, trustworthiness, or good judgment.

I also find that Applicant has mitigated the security significance of his conduct under this guideline. There is no doubt that Applicant and Company A did not part on good terms. That is shown by the voluminous legal records provided by Applicant. He reasonably viewed his conduct as innocuous and allowable. Applicant admitted that his conduct could have been viewed negatively. However, the evidence is insufficient to show that it was untrustworthy, or showed sufficient poor judgment as to justify denial of national security eligibility. While, arguably, his conduct could be seen as violating the PIAIA, it is vitiated by its minor nature and the time period since such conduct occurred.

Whole-Person Concept

Under the whole-person concept, the administrative judge must evaluate an applicant's eligibility for national security eligibility 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(d):

(1) the nature, extent, and seriousness of the conduct; (2) the circumstances surrounding the conduct, to include knowledgeable participation; (3) the frequency and recency of the conduct; (4) the individual's age and maturity at the time of the conduct; (5) the extent to which participation is voluntary; (6) the presence or absence of rehabilitation and other permanent behavioral changes; (7) the motivation for the conduct;

(8) the potential for pressure, coercion, exploitation, or duress; and (9) the likelihood of continuation or recurrence.

Under AG ¶ 2(c), the ultimate determination of whether to grant national security 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 pertinent facts and circumstances surrounding this case. Applicant has mitigated the concerns surrounding his alleged misuse of information technology, and related personal conduct. There is little to no potential for pressure, coercion, or duress, and little likelihood of recurrence. Overall, the record evidence does not create substantial doubt as to Applicant's present suitability for national security eligibility, and a security clearance.

Formal Findings

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

Paragraph 1, Guideline M:	FOR APPLICANT
Subparagraph 1.a:	For Applicant
Paragraph 2, Guideline E:	FOR APPLICANT
Subparagraph 2.a:	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 or continue Applicant's national security eligibility for a security clearance. Eligibility for access to classified information is granted.

WILFORD H. ROSS
Administrative Judge