DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ADP Case No. 17-03023
	)	
Applicant for Public Trust Position	)	

Appearances

For Government: Brian Olmos, Esq., Department Counsel
For Applicant: Tod D. Stephens, Esq.

06/04/2019

_____

Decision

_____

COACHER, Robert E., Administrative Judge:

The Government failed to establish the foreign influence, under Guideline B, or the personal conduct, under Guideline E, concerns against Applicant. Alternatively, Applicant mitigated the foreign influence and personal conduct trustworthiness concerns. Applicant's eligibility for a position of trust is granted.

Statement of the Case

On March 7, 2018, the Department of Defense Consolidated Adjudications Facility (DOD CAF) issued Applicant a Statement of Reasons (SOR) detailing trustworthiness concerns under Guidelines B and E. DOD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the adjudicative guidelines implemented on June 8, 2017 (AG).

Applicant answered (Ans.) the SOR on March 30, 2018, and requested a hearing before an administrative judge. On April 4, 2019, the case was assigned to me. On April

25, 2019, the Defense Office of Hearings and Appeals (DOHA) notified Applicant that the hearing was scheduled for May 23, 2019. I convened the hearing on that date. Government exhibits (GE) 1-14 were admitted in evidence without objection. The exhibit list was marked as hearing exhibit (HE) I. The Government's request for administrative notice was marked as HE II. Applicant testified, presented three witnesses, and offered exhibits (AE) A-RR, which were admitted without objection. DOHA received the transcript (Tr.) on June 3, 2019.

Procedural Rulings

I took administrative notice of facts concerning Russia. Department Counsel provided supporting documents that verify, detail, and provide context for the requested facts. The specific facts noticed are included in the Findings of Fact.

Administrative or official notice is the appropriate type of notice used for administrative proceedings. (See ISCR Case No. 05-11292 at 4 n.1 (App. Bd. Apr. 12, 2007); ISCR Case No. 02-24875 at 2 (App. Bd. Oct. 12, 2006) (citing ISCR Case No. 02-18668 at 3 (App. Bd. Feb. 10, 2004) and *McLeod v. Immigration and Naturalization Service*, 802 F.2d 89, 93 n.4 (3d Cir. 1986)) Usually administrative notice in ISCR proceedings is accorded to facts that are either well known or from U.S. Government reports. (See Stein, Administrative Law, Section 25.01 (Bender & Co. 2006) (listing fifteen types of facts for administrative notice))

Findings of Fact

In Applicant's answer to the SOR, she admitted one of the allegations, with explanations (SOR 2.a). She denied the remaining two allegations (SOR 1.a and 2.b). Her admission is incorporated into the findings of fact. After a thorough and careful review of the evidence, I make the following additional findings of fact.

Applicant is 61 years old. She has worked for her current federal contractor-employer for approximately 20 years, on and off. She is a software development project manager. She holds bachelor's and MBA degrees. She is a native-born U.S. citizen and has always resided in this country. She has lived in her current location for over 30 years. She has been married over 30 years and has two adult sons. She previously held a public trust position when she worked for another government agency. (Tr. at 26-27, 30-31, 33; GE 1.)

The SOR alleged that Applicant's former employment as the vice president of government sector systems engineering with Company 1 (C1), a company with ties to Russian intelligence and the Russian government, created a conflict of interest and a heightened risk of exploitation (SOR 1.a); the SOR also alleged that Applicant maintained her employment with C1 from March 2014 through January 2015 despite knowing that C1 may be affiliated with the Russian government or Russian intelligence, and that her former employment with C1 creates an ongoing potential for a conflict of interest and could create an increased security risk (SOR 2.a-2.b).

Sometime before March 2014, a former coworker of Applicant's reached out to her to see if she would be interested in a position with a new company (C1) for which he was the general manager. Applicant understood C1 to be a services company, which "sold" its customers consulting support. C1 was a registered U.S. company. Its parent company was C2 and was also a U.S. registered company. C2's parent company was C3, which was identified as a Russian company. C2 and C3 were software sales companies. C1 did not sell software. Applicant accepted the position and was hired in March 2014 as the Vice President, Government Sector Systems Engineering. Her salary was approximately $165,000 per year, up from approximately $135,000 that she earned from her last employer. Since C1 was a brand new company with no existing clientele, the first several months of the job entailed Applicant setting up and organizing the office. At the time, C1 had a total of four employees: the general manager, Applicant, another vice president who served as the general manager's deputy, and an office manager who had the title of operations manager. (Tr. at 37-40, 42; Ans.; GE 2; AE A)

Applicant credibly testified that while she worked for C1 it was unable to secure any contracts. She believed that C1 was funded by C2 or C3 during this time, although she had no personal involvement with C2 or C3. Her general manager required Applicant to attend C3's annual meeting in June 2014, which was held in Russia. Applicant was there to attend events, she was not a presenter or speaker. Her general manager made presentations at some seminars. She did not make any acquaintances at this meeting. Applicant became concerned about working for C1 when her general manager told her of an encounter he had during the Russia meeting. The general manager stated that he was invited into the office of someone and noticed a uniform on display. He recognized it as a possible former KGB (former Soviet secret intelligence service) uniform. In July 2014 when Applicant got back to the United States and thought about this disclosure by her general manager, she decided to quit working for C1. She did not actually quit the job until December 2014 and stopped being paid in January 2015. She explained this delay was because she was also teaching as an adjunct professor at a local university at the time, which did not allow her time to search for a new job. She was advised early on in her working career to never quit a job until she had another job lined up. Her family circumstances at the time were that she was paying for her two son's college tuitions and her health insurance was through C1. She was able to secure follow-on employment in February 2015. Shortly after she left the company, the general manager was let go from his position and C1 stopped doing business. (Tr. at 43-49, 56-59, 73-74; Ans.; GE 2)

In October 2014, while still employed by C1, Applicant attended a government cybersecurity forum in the United States. She participated as a panelist. The founder and CEO of C3 authored the written welcome page to the forum's written materials, but he was not in attendance. The forum was attended by current and former U.S. government officials. (Tr. at 69-70; GE 3)

In September 2017, The Department of Homeland Security (DHS) issued a binding operational directive (BOD), applicable to all federal agencies, to remove and

discontinue use of any products associated with C1, C2, and C3 because of the risk those products create to federal information and information systems. (See 44 U.S.C. § 3552(b)) This BOD became a final decision in December 2017. Applicant quit working for C1 approximately two and a half years before the issuance of the BOD. Except when the operations manager called Applicant in February 2015 to tell her she was leaving C1, Applicant has had no contact with C1, C2, or C3, or its former employees since she quit. She has no family or friends in Russia. She has never had any contacts with any member of the Russian government. Her only trip to Russia was in June 2014 while working for C1. (Tr. at 63, 72, 74, 79; GE 6-10; AE K)

Applicant admitted her employment with C1 when completing her trustworthiness application and during her interview with a defense investigator. She lists this employment on her resume and on her employment-related social media page. She has never attempted to conceal her employment with C1 from the government. (Tr. at 29, 83; AE 1-2, 4)

Applicant documented her financial and community ties to the United States. Her home value is approximately $385,000, with approximately $102,000 worth of equity. Her U.S. investments and insurance total approximately $583,000. She is an active member in her local church, sings in a community choir, participates in Habitat for Humanity events, donates blood to the Red Cross, and volunteered to help at a local shelter. She is a registered voter in her home state and has exercised her right to vote on a regular basis. (Tr. at 76-78, 80-81; AE E-J, S-Y)

Character Evidence.

Applicant presented the testimony of three character witnesses. Witness one (W1) is Applicant's sister-in-law and has known her for 40 years. W1 also worked for a government agency for 39 years as a senior executive and held a top secret clearance with sensitive access. Her background and experience has given her specialized insight to foreign companies trying to exploit U.S. companies for sensitive information. She is also aware of the allegations in Applicant's SOR. She was aware of Applicant's employed with C1 in 2014 and became aware of Applicant's disillusionment with her employment after returning from Russia. Applicant's values were not the same as those held by C1. W1 has not witnessed or been apprised of any follow-on contacts between Applicant and C1, C2, or C3. W1 believes Applicant has strong loyalties to the United States and would trust her with sensitive or classified information. W1 also provided a sworn affidavit (Tr. at 116-125; AE BB)

Witness two (W2) currently works with Applicant. He is the lead security person on the DOD contract for his employer and has worked industrial security issues for 15 years. He has also served as the facilities security officer (FSO). Part of his duties included overseeing the company's insider threat program. He has held a security clearance for 17 years. He also worked for the U.S. Secret Service for two years. Applicant has always completed her security training on time. Applicant "complies with our security program and company security rules and has never been the cause of any

security problems." Applicant has never demonstrated any behavior that would lead W2 to question her personal integrity or loyalty to this country. W2 also supplied a sworn affidavit. (Tr. at 128-134; AE AA)

Witness three (W3) has known Applicant for 30 years and is a close personal friend. W3 is an in-house legal counsel to a defense contractor and holds a security clearance. She is aware of the allegations in Applicant's SOR. Applicant has never shared any work-related sensitive information with W3. Applicant is unquestionably trustworthy and does what is right. W3 also supplied a sworn affidavit. (Tr. at 136-143; AE R)

Applicant also provided the sworn affidavits of 19 other persons who are (or were) coworkers and friends. All universally opined that she is reliable, responsible, and trustworthy. (AE N-Q, CC-QQ)

Administrative Notice-Russia.

Russia has a highly centralized, weak multi-party political system dominated by the president. Russia has significant human-rights problems, marked by restrictions on civil liberties, discrimination, denial of due process, forced confessions, torture, other prisoner mistreatment, and the government's failure to prosecute officials who commit serious violations. Government officials also engage in electronic surveillance without proper authorization.

Russia is one of the most aggressive countries conducting espionage against the United States, focusing on obtaining proprietary information and advance weapons technologies beneficial to Russia's military modernization and economic development. Russia's intelligence services as well as private companies and other entities frequently seek to exploit Russian citizens or persons with family ties to Russia who can use their insider access to corporate networks to steal secrets. They also have offered financial inducements to U.S. government officials and citizens to encourage them to compromise classified information. Russia's attempts to collect U.S. technological and economic information represent a growing and persistent threat to U.S. security. (HE II)

Policies

When evaluating an applicant's suitability for a public trust position, the administrative judge must consider the disqualifying and mitigating conditions in the AG. 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(a), 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 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. 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 as to obtaining a favorable trustworthiness decision.

A person who seeks access to sensitive 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 sensitive information. Decisions include, by necessity, consideration of the possible risk the applicant may deliberately or inadvertently fail to protect or safeguard sensitive information. Such decisions entail a certain degree of legally permissible extrapolation as to potential, rather than actual, risk of compromise of sensitive information.

Section 7 of EO 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 B, Foreign Influence

AG 6 explains the trustworthiness concern about "foreign contacts and interests" as follows:

> Foreign contacts and interests, including, but not limited to, business, financial, and property interests, are a national security concern if they result in divided allegiance. They may also be a national security concern if they create circumstances in which the individual may be manipulated or induced to help a foreign person, group, organization, or government in a way inconsistent with U.S. interests or otherwise made vulnerable to pressure or coercion by any foreign interest. Assessment of foreign contacts and interests should consider the country in which the foreign contact or interest is located, including, but not limited to, considerations

such as whether it is known to target U.S. citizens to obtain classified or sensitive information or is associated with a risk of terrorism.

AG 7 indicates conditions that could raise a trustworthiness concern and may be disqualifying in this case:

> (a) contact, regardless of method, with a foreign family member, business or professional associate, friend, or other person who is a citizen of or resident in a foreign country if that contact creates a heightened risk of foreign exploitation, inducement, manipulation, pressure, or coercion; and
>
> (b) connections to a foreign person, group, government, or country that create a potential conflict of interest between the individual's obligation to protect classified or sensitive information or technology and the individual's desire to help a foreign person, group, or country by providing that information or technology.

Applicant was hired by C1 in 2014 and worked for it for approximately 11 months. She quit in January 2015. In September 2017, C1 (along with its parent companies C2 and C3) was a subject of BOD 17-01, which required all U.S. government agencies to rid themselves of any products or services rendered by these companies. The BOD was issued because of the companies' possible affiliation with Russia and Russian intelligence services. Applicant has no further ties to C1 (and never had any direct ties to C2, or C3), has no family, friends, or other contacts with Russia or the Russian government. The Government failed to establish an existing connection between Applicant and any Russian interest. AG 7(a) and 7(b) have not been established by substantial evidence.

Although my findings lead to the conclusion that the foreign influence concerns were not established, I also find that the evidence would support the application of mitigating conditions to Applicant's case.

AG 8 lists conditions that could mitigate foreign influence trustworthiness concerns, including:

> (a) the nature of the relationships with foreign persons, the country in which these persons are located, or the positions or activities of those persons in that country are such that it is unlikely the individual will be placed in a position of having to choose between the interests of a foreign individual, group, organization, or government and the interests of the U.S.; and
>
> (b) there is no conflict of interest, either because the individual's sense of loyalty or obligation to the foreign person, or allegiance to the group, government, or country is so minimal, or the individual has such deep and longstanding relationships and loyalties in the United States, that the

individual can be expected to resolve any conflict of interest in favor of the U.S. interest.

Applicant credibly testified that she had no contact with any Russian entity and quit working for C1 in 2015, long before the BOD was even issued. She presented sufficient evidence to establish that it is unlikely that she would be placed in a position to choose between the interest of Russia and those of the United States. She has no connection to Russia or the Russian government. AG ¶ 8(a) applies.

Applicant has met his burden to establish her "deep and longstanding relationships and loyalties in the U.S." She is a native-born citizen, has resided her whole life in the United States, and has family, community and financial interests only in the United States. There is no evidence on any interests in Russia. Friends and co-workers attest to her loyalty, dedication, and overall trustworthiness. The evidence supports that Applicant has longstanding ties to the United States and would resolve any conflict of interest in favor of the United States. AG ¶ 8(b) applies.

Guideline E, Personal Conduct

AG 15 expresses the personal conduct trustworthiness 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 or sensitive information. Of special interest is any failure to cooperate or provide truthful and candid answers during national security investigative or adjudicative processes. . . .

AG 16 describes conditions that could raise a trustworthiness concern and may be disqualifying in this case. The following disqualifying conditions are potentially applicable:

> (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 individual may not properly safeguard classified or sensitive information; and
>
> (d) credible adverse information that is not explicitly covered under any other guideline and may not be sufficient by itself for an adverse determination, but which, when combined with all available information supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the

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

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

(2) disruptive, violent, or other inappropriate behavior in the workplace;

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

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

Applicant's employment by C1, and subsequent quitting the company, nearly three years before the U.S. Government determined that C1 posed a security problem does not establish a trustworthiness concern under AG 16(c) or 16(d). Applicant has been forthcoming about her employment relationship with C1, which ended in January 2015. Applicant has no further connection to the company. The Government suggests that Applicant should have reacted quicker in leaving C1 when she became concerned after her trip to Moscow and that she should have reported her suspicions to someone in authority. The time she took to leave the company was reasonable since she needed to secure other employment to maintain her lifestyle. She had no duty to report the information that came to her by hearsay about whether a possible former KGB agent worked for C2 or C3. Finally, the U.S. Government apparently contracted with C2 and C3 and did not become concerned about that vulnerability until September 2017, long after Applicant had divested herself of employment with C1.

Although my findings lead to the conclusion that the personal conduct concerns were not established, I also find that the evidence would support the application of mitigating conditions to Applicant's case.

I have also considered all of the mitigating conditions for personal conduct under AG 17 and considered the following relevant:

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

Since Appellant is no longer employed or affiliated with C1, C2, or C3 it is unlikely that she will have any future contact with any of the companies. Applicant's reliability, trustworthiness, and good judgment were not impacted by her brief employment with C1, which was before it was a known concern to the U.S. Government. AG 17(c) applies.

Whole-Person Concept

Under the whole-person concept, the administrative judge must evaluate an applicant's eligibility for a trustworthiness determination by considering the totality of the applicant's conduct and all the 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 eligibility for access to sensitive information 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. The circumstances tending to support granting Applicant's eligibility for access to sensitive information are more significant than the factors weighing towards denying her eligibility for access to sensitive information. I considered the recommendations of her co-workers and supervisors, who resoundingly recommend that Applicant be granted her trustworthiness determination. I also considered her strong ties to this country. She has demonstrated her longstanding loyalty to the United States, as well as her reliability, trustworthiness, and good judgment. Even though the Government failed to establish any trustworthiness concerns, she also provided sufficient evidence to mitigate any of those concerns.

Overall the record evidence leaves me without questions or doubts as to Applicant's eligibility and suitability for access to sensitive information. For all these reasons, I conclude that the trustworthiness concerns arising under Guideline B, foreign influence, and Guideline E, personal conduct, were either not established or were mitigated.

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 B:	FOR APPLICANT
Subparagraph 1.a:	For Applicant

Paragraph 2, Guideline E:	FOR APPLICANT
Subparagraphs 2.a - 2.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 access to sensitive information. Eligibility for access to sensitive information is granted.

_____
Robert E. Coacher
Administrative Judge