DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 16-03472
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Daniel Crowley, Esq., Department Counsel
For Applicant: William F. Savarino, Esq.

12/27/2018

Decision

GARCIA, Candace Le'i, Administrative Judge:

Applicant did not mitigate the personal conduct, use of information technology, and foreign influence security concerns. Eligibility for access to classified information is denied.

Statement of the Case

On February 14, 2017, the Department of Defense (DOD) issued a Statement of Reasons (SOR) to Applicant detailing security concerns under Guideline E (personal conduct), Guideline M (use of information technology), and Guideline B (foreign influence). The action was taken under Executive Order (Exec. Or.) 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; DOD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the adjudicative guidelines (AG).[1]

[1] I decided this case using the AG implemented by DOD on June 8, 2017. However, I also considered this case under the previous AG implemented on September 1, 2006, and my conclusions are the same using either set of AG.

Applicant responded to the SOR on March 15, 2017, and requested a hearing. The case was assigned to me on November 9, 2017. The Defense Office of Hearings and Appeals (DOHA) issued a notice of hearing (NOH) on December 8, 2017, scheduling the hearing for January 22, 2018. A notice of cancellation for that hearing was issued on January 19, 2018, due to the U.S. Government shutdown. A second NOH was issued on April 9, 2018, scheduling the hearing for May 18, 2018. I convened the hearing as scheduled.[2]

I marked the Government's discovery letter, request for administrative notice, and exhibit list as Hearing Exhibits (HE) I, II, and III, and Applicant's exhibit list as HE IV. Government Exhibits (GE) 1 through 5 were admitted in evidence without objection. Applicant testified, called one witness, and submitted Applicant's Exhibits (AE) A through N, which were admitted in evidence without objection. DOHA received the hearing transcript (Tr.) on June 6, 2018.

Findings of Fact

Applicant admitted the allegations in SOR ¶¶ 1.a, 3.a, 3.b, and 3.c. He denied SOR ¶¶ 1.b and 2.a. He is 50 years old. He married in 2000, divorced in 2009, and remarried in 2010. He has four minor children. All are native-born U.S. citizens. His eldest child is from a prior relationship. His second child is from his prior marriage. His youngest two children are from his current marriage.[3]

Applicant graduated from high school in 1986. He earned a bachelor's degree in 1990 and a master's degree in 2002. He served in the U.S. Navy from 1990 to 1994, when he was honorably discharged. He has since worked for various defense contractors. As of the date of the hearing, he worked as a senior engineer for his current employer, for whom he has worked since late February 2015. He previously worked for the same company from June 2007 to February 2009. He was first granted a security clearance in 1990.[4]

Applicant's wife was born in Russia. She is 33 years old. She earned a bachelor's and a master's degree from a university in Russia in around 2002 and 2009, respectively. She first immigrated to the United States in 2004. She then returned to Russia, where she married her first spouse, who was then a Russian citizen, in 2005. Her first spouse is now a U.S. citizen residing in the United States. They immigrated to the United States in 2005 and divorced in 2007. She remarried a Ukrainian national in 2009 and they lived together in the United States. She then returned to Russia in 2009 for one month to finish her master's degree, after which time she returned to the United States. She divorced her second spouse in 2010.[5]

[2] Tr. at 7-8.

[3] Response to the SOR; Tr. at 36, 39-41, 75, 77, 85; GE 1, 2; AE D, K, N.

[4] Tr. at 36-39, 43-51, 97-98; GE 1, 2; AE A, D, F.

[5] Tr. at 78-90, 94-97, 105-112; GE 1, 2; AE B, D, K, L, M, N.

Applicant's wife became a naturalized U.S. citizen in 2014. She renounced her Russian citizenship in 2016. She has worked as a business financial manager for an engineering firm since May 2015. The company's partner, who is also the facility security officer (FSO), indicated that while Applicant's wife does not need a security clearance, she has received security training like those who do. He described her as a valued and trusted employee who safeguards the company's confidential, sensitive, and proprietary information. He also indicated that she appears to be a loyal American citizen.[6]

Applicant's parents-in-law and brother-in-law are citizens and residents of Russia. His parents-in-law divorced in 2010. His father-in-law is 60 years old. Applicant testified that his wife's father is estranged from the family. She talks to her father several times yearly, and she has seen him three times between 2008 and 2018. Her father met her during one of her trips to Russia so that he could meet his grandson. Applicant has never met or talked to his father-in-law. Applicant is unaware whether his father-in-law is currently employed, and his wife believes her father is retired. Applicant's father-in-law is a former Russian military officer. Applicant testified that his father-in-law served in the Russian military for several years from around 1983 to 1985, before he was discharged for stealing rubbing alcohol.[7]

Applicant's mother-in-law is 60 years old. She works as an accountant for a brewery. His brother-in-law is 24 years old. After Applicant's brother-in-law graduated from college, he completed one year of mandatory service in the Russian military in around December 2017. He works as a chemist for a private pharmaceutical company. Applicant was unaware if his brother-in-law had any ongoing affiliations with the Russian government or military. Applicant's wife video chats with her mother once weekly. She is close to her brother and talks to him more frequently, at least several times weekly and most recently because of his imminent wedding. His mother-in-law speaks "very little" English and Applicant speaks "very little" Russian, so he simply says "hello" and ensures that his children do the same on the occasions that his wife talks to her mother. He has a similar relationship with his brother-in-law.[8]

Applicant traveled to Russia in 2010, 2011, 2013, and 2014. He followed security clearance protocol and reported such travels to his FSO. His wife travels to Russia once yearly, and she stays with her mother during such visits. Though Applicant planned to travel to Russia with his family to attend his brother-in-law's wedding and celebrate his 50th birthday, he elected not to do so while his clearance decision was pending. His wife and two children planned to attend her brother's wedding in Russia, where they would stay in a condominium paid for by her brother. His mother-in-law and brother-in-law have visited and stayed with them in the United States. They did so before Applicant and his wife married, and his mother-in-law did so again after the birth of their son in

[6] Tr. at 78-90, 94-97, 105-112; GE 1, 2; AE B, D, K, L, M, N.

[7] Tr. at 78-90, 94-97, 105-112; GE 1, 2; AE D, L, M, N.

[8] Tr. at 78-90, 94-97, 105-112; GE 1, 2; AE D, L, M, N.

2013 for six months. She has attempted to revisit them since but her visa has been denied at least three times.[9]

In around 2013, Applicant's mother-in-law sold her condominium in Russia, and gave $90,000 of the proceeds to Applicant and his wife, which they used as a deposit for their home in the United States. Applicant reported this monetary gift to his FSO. They have not received any additional money and his wife does not have standing to inherit any money from anyone in Russia. They do not have any assets, obligations, or affiliations in Russia. Their assets in the United States total around $1,840,000.[10]

Applicant's in-laws in Russia are aware that he works as an engineer. He has not told them that he holds a security clearance or works on U.S. Government contracts. He is unaware if his wife has ever disclosed this information to them; she indicated that she has not shared information about Applicant's work or need for a clearance to any foreign national, to include her mother and brother. Applicant is unaware whether his in-laws in Russia have ever been approached by anyone in the Russian government or military seeking information about him or his employment. He testified that he would report to his FSO and the proper authorities any attempts by anyone in Russia to blackmail him.[11]

Applicant looked at pornography on his work computer from around February 2014 through February 2015. At the time, he had been working for a subcontractor since 2008. He attributed his actions to the "gross miscalculation" he made as a result of an "extreme amount of stress" from 2013 through 2015. His eldest child was born in 2013 with a medical condition requiring multiple surgeries through 2015, as well as continuous checkups every six months indefinitely. He described this experience as a "traumatic" one. In addition, he and his wife "were not in a good spot at all" after she had disclosed to him that she had multiple affairs between 2013 and 2015.[12]

Initially, Applicant only looked at pornography at home. When he became addicted to it, he also looked at pornography at work. He testified that pornography:

> [w]as my outlet, that was my release. Whether it was five, ten minutes, you know, before work started. Ten, 20, 30 minutes after work . . . before I went home . . . It relaxed me. It prepared me for going home and having to work through everything that was going on in the house.

He also acknowledged that he looked at pornography at work at lunch time. He estimated that he looked at pornography at work an average of 15 to 30 minutes daily.

[9] Tr. at 78-90, 94-97, 105-112; GE 1, 2; AE D, L, M, N.

[10] Tr. at 78-90, 94-97, 105-112; GE 1, 2, 5; AE A, D, E, L, M, N.

[11] Tr. at 78-90, 94-97, 105-112; GE 1, 2, 5; AE A, D, E, L, M, N.

[12] Tr. at 36-77, 90-93, 98-99; GE 1, 2, 3, 4, 5; AE G, N.

He maintained that it never interfered with his work. He did not tell anyone at the time that he was looking at pornography at work because he knew it was improper.[13]

In early February 2015, the primary defense contractor removed Applicant from the U.S. Government contract to which he had been assigned through his subcontractor company. His program manager informed him that computer monitoring revealed that he had been accessing pornography on his work computer. He immediately reported his removal and the reason for his removal to his company's President, Vice President, and FSO. He was placed on administrative leave by his company during the two-week period in which the primary contractor conducted its investigation, then he was terminated by his company in around mid-February 2015.[14]

The investigation conducted by the primary contractor, summarized in an April 2, 2015 letter, consisted of a forensic examination of Applicant's computer, an interview of the contract's technical lead, and a review of Applicant's time sheets, contract documents, and internet logs. Applicant was never interviewed. The investigation determined that Applicant viewed pornography during periods that were billed to the U.S. Government. As such, the primary contractor indicated that it would issue to the U.S. Government a credit of $21,577.[15]

Applicant denied that he ever mischarged to the government contract any time in which he looked at pornography at work. He testified that he was aware that the primary defense contractor paid $20,000 to the U.S. Government agency in association with his alleged mischarging; his company repaid the primary contractor $20,000 at the latter's request; he was unaware how the amount of $20,000 was quantified; and he was never asked to repay any money. He acknowledged during his July 2016 background interview that the $20,000 was restitution for an established 100 hours of computer use during work hours for personal purposes. A May 2016 letter memorializing a meeting between Applicant, his attorney, and debarment officials, reflects that "it was clear that [Applicant] has accepted responsibility for mischarging a government contract for misspent time."[16]

Applicant was placed under surveillance for one year by his company's ethics committee from 2016 to 2017. He was required to report his time and his computer was monitored, as further discussed below. He has had no other unfavorable issues. He testified that it was not easy for him to stop looking at pornography at work. Once he was terminated by his prior company, he sought help for the first time. He voluntarily attended multiple Sex Addicts Anonymous (SAA) meetings for two and a half years to address his addiction. He no longer feels he is addicted to pornography, he intends to continue to attend SAA meetings in the future, and he does not intend to look at

[13] Tr. at 36-77, 90-94, 98-101; GE 2, 3, 4, 5.

[14] Tr. at 36-77, 90-93, 98-101; GE 1, 2, 3, 4, 5; AE A, F, G, H, I.

[15] Tr. at 56-77, 90-94, 98-101; GE 2, 3; AE H, I, J.

[16] Tr. at 36-77, 90-94, 98-104, 113-115; GE 1, 2, 3; AE A, F, G, H, I, J.

pornography on his work computer in the future. He eventually disclosed his conduct of viewing pornography at work and his consequent termination to his wife, who supports his SAA attendance and has herself attended such meetings. He handles stress by working out, playing games on his phone, and keeping busy with his family.[17]

Applicant's character witness was a vice president for the defense contractor for whom they worked. He was also Applicant's division director and direct supervisor of three years. He has held a security clearance at various occasions over a 30-year-period. Though the witness was not involved in rehiring Applicant, he testified that Applicant had self-reported his issue with his prior defense contracting company to both the witness and his predecessor, and despite such knowledge, the predecessor chose to rehire Applicant. He testified that he was aware that Applicant viewed pornography on his work computer during his off hours while employed by the prior defense contractor; he self-reported his conduct to his then-employer; and Applicant had to leave that company after he was consequently removed from the contract. The witness testified that he was unaware that any allegations were ever substantiated concerning Applicant mischarging his prior employer for time associated with his pornography usage at work.[18]

The witness testified that he discussed the matter with an individual from Applicant's prior employer, who described Applicant's conduct as a mistake and indicated that Applicant had otherwise been trustworthy. The witness also testified that he discussed the matter directly with Applicant and brought it to the attention of their employer's ethics committee. The committee, noting that Applicant did not have any unfavorable issues during his previous employment with their company, placed Applicant on a one-year observation period beginning in around July 2016, which coincided with Applicant's proposed debarment period.[19]

During this time, Applicant reported his time to the witness daily, his computer access was monitored, and the government contractor to which he was assigned was asked to provide any relevant observations. At the year's conclusion, the committee determined that there was no longer a need for further observation of Applicant and the proposed debarment had also ended. Applicant continued, however, to report to the witness. The witness has received favorable reports of Applicant's performance, and rated Applicant outstanding in his performance evaluations. He testified that Applicant has complied with annual security and ethics trainings, and he considers Applicant trustworthy, of good judgment, and capable of following rules and regulations. Applicant's FSO since 2010 described Applicant as an individual who follows security rules and procedures. His FSO also indicated that Applicant has completed his annual security training requirements. [20]

[17] Tr. at 36-77, 90, 98, 104-105, 112-113; GE 1, 2, 4; AE C, G, I, N.

[18] Tr. at 17-35.

[19] Tr. at 17-35.

[20] Tr. at 17-35; AE A.

Russia

In 2016, Russia continued to be a leading state intelligence threat to U.S. interests. Its intelligence services target U.S. and allied personnel with access to sensitive computer network information. It is assuming a more assertive cyber posture based on its willingness to target critical infrastructure systems and conduct espionage operations, even when detected and under increased public scrutiny. It has developed a ground-launched cruise missile that the United States has declared is in violation of the Intermediate-Range Nuclear Forces Treaty.

Russia remains one of the top two most aggressive and capable collectors of sensitive U.S. economic information and technologies, particularly in cyberspace. Non-cyberspace collection methods include targeting of U.S. visitors overseas, especially if the visitors are assessed as having access to sensitive information. Russia's highly capable intelligence services are using human intelligence gathering, cyber, and other operations to collect economic information and technology to support its economic development and security. It continues to take information warfare to a new level, working to fan anti-U.S. and anti-Western sentiment both within Russia and globally.

The most significant human rights problems in Russia in 2015 involved restrictions on the ability to choose one's government and freedoms of expression, assembly, association, and the media, as well as internet freedom; political prosecutions and administration of justice; and government discrimination against racial, ethnic, religious, and sexual minorities. Other problems included allegations of torture and excessive force by law enforcement officials; executive branch pressure on the judiciary; electoral irregularities; and extensive official corruption. The government failed to take steps to prosecute or punish most officials who committed abuses.

Although Russian law prohibits officials from entering a private residence except in cases prescribed by federal law or when authorized by a judicial decision, government officials entered residences and premises without warrants. While Russian law also prohibits government monitoring of correspondence, telephone conversations, and other means of communication without a warrant, government officials engaged in electronic surveillance without appropriate authorization.

In October 2016, the U.S. Department of Homeland Security (DHS) and Office of the Director of National Intelligence (ODNI) issued a Joint Statement on Election Security, stating that the U.S. intelligence community was confident that the Russian government directed recent compromises of emails from U.S. persons and institutions, including from U.S. political organizations. In December 2016, the DHS, ODNI, and the Federal Bureau of Investigation released a Joint Analysis Report stating that activity by Russian intelligence services has been part of a decade-long campaign of cyber-enabled operations directed at the U.S. Government and its citizens. The campaign included spear phishing; targeting of government organizations, critical infrastructure, think tanks, universities, political organizations, and corporations; theft of information from these organizations; and the recent public release of some of this stolen information.

Policies

When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the adjudicative guidelines. In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially disqualifying conditions and mitigating conditions, which are to be 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, administrative judges apply the 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(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."

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 the applicant or proven by Department Counsel." The applicant has the ultimate burden of persuasion 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 safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation of potential, rather than actual, risk of compromise of classified information.

Section 7 of Exec. Or. 10865 provides that adverse 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* Exec. Or. 12968, Section 3.1(b) (listing multiple prerequisites for access to classified or sensitive information).

Analysis

Guideline E, Personal Conduct

AG ¶ 15 expresses the security concern for personal conduct:

> 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 security concern and may be disqualifying. I considered the following relevant:

> (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;
>
> (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. 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 government protected information;
> >
> > (2) any disruptive, violent, or other inappropriate behavior;
> >
> > (3) a pattern of dishonesty or rule violations; and
> >
> > (4) evidence of significant misuse of Government or other employer's time or resources; and
>
> (e) personal conduct, or concealment of information about one's conduct, that creates a vulnerability to exploitation, manipulation, or duress by a foreign intelligence entity or other individual or group. Such conduct includes:

(1) engaging in activities which, if known, could affect the person's personal, professional, or community standing.

Applicant looked at pornography on his work computer from around February 2014 through February 2015. He estimated at the hearing that he looked at pornography at work an average of 15 to 30 minutes daily. He did not tell anyone at the time that he was looking at pornography at work because he knew it was improper. While he denied that he ever mischarged to the government contract any time in which he looked at pornography at work, the investigation conducted by the primary defense contractor concluded that he had. The primary contractor paid $21,577 to the U.S. Government for Applicant's mischarged time and his then-employer had to repay the money to the primary contractor. He acknowledged during his July 2016 background interview that the $20,000 was restitution for an established 100 hours of computer use during work hours for personal purposes. Finally, the letter memorializing his meeting with the debarment officials indicates that he accepted responsibility for mischarging a government contract for misspent time. AG ¶¶ 16(c), 16(d), and 16(e) apply.

I have considered all of the mitigating conditions 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; and

(d) 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 contributed to untrustworthy, unreliable, or other inappropriate behavior, and such behavior is unlikely to recur.

Applicant's conduct of viewing pornography on his work computer daily from February 2014 through February 2015 was a serious offense. He immediately acknowledged his conduct once it was discovered through computer monitoring, and he then immediately reported such conduct to his then-employer as well as his current employer. He complied with all requirements imposed on him by his current employer and he has not had any other unfavorable issues. He attended SAA meetings, and he disclosed his conduct and consequent termination to his wife.

Applicant has not, however, taken full responsibility for his conduct. Again, he denied that he ever mischarged the government contract to which he was assigned for time spent viewing pornographic material on his work computer. Yet, the investigation conducted by the primary defense contractor concluded that he had. Moreover, the letter memorializing his meeting with the debarment officials clearly states that he had accepted such responsibility. As such, his reliability, judgment, and trustworthiness remain questionable. I find that AG ¶¶ 17(c) and 17(d) are not established.

Guideline M, Use of Information Technology

AG ¶ 39 expresses the security concern for use of information technology:

> 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. 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 these operations.

AG ¶ 40 describes conditions that could raise a security concern and may be disqualifying. I considered the following relevant:

(e) unauthorized use of any information technology system.

Applicant looked at pornography on his work computer from around February 2014 through February 2015. He did not tell anyone at the time that he was looking at pornography at work because he knew it was improper. AG ¶ 40(e) applies.

I have considered all of the mitigating conditions under AG ¶ 41 and considered the following relevant:

> (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.

For the same reasons set forth above in my Guideline E analysis, I find that AG ¶ 41(a) is not established.

Guideline B, Foreign Influence

AG ¶ 6 expresses the security concern for foreign influence:

> 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 describes conditions that could raise a security concern and may be disqualifying. I considered the following relevant:

> (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;
>
> (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; and
>
> (e) shared living quarters with a person or persons, regardless of citizenship status, if that relationship creates a heightened risk of foreign inducement, manipulation, pressure, or coercion.

The nature of a nation's government, its relationship with the United States, and its human rights record are relevant in assessing the likelihood that an applicant's family members are vulnerable to government coercion. The risk of coercion, persuasion, or duress is significantly greater if the foreign country has an authoritarian government, a family member is associated with or dependent upon the government, or the country is known to conduct intelligence operations against the United States. In considering the nature of the government, an administrative judge must also consider any terrorist activity in the country at issue. *See generally* ISCR Case No. 02-26130 at 3 (App. Bd. Dec. 7, 2006) (reversing decision to grant clearance where administrative judge did not consider terrorist activity in area where family members resided).

AG ¶ 7(a) requires substantial evidence of a "heightened risk." The "heightened risk" required to raise one of these disqualifying conditions is a relatively low standard. "Heightened risk" denotes a risk greater than the normal risk inherent in having a family member living under a foreign government.

Applicant's parents-in-law and brother-in-law are citizens and residents of Russia, and his father-in-law is a former officer in the Russian military. While Applicant testified that his father-in-law is estranged from the family, his wife talks to her father several times yearly and she saw him in Russia so that he could meet his grandson. Applicant's wife is close to her mother and brother. She talks to them frequently. She visits them in Russia once yearly, and she most recently traveled to Russia in 2018 for her brother's wedding.

Russia is one of the leading state intelligence threats to U.S. interests. It remains one of the top two most aggressive and capable collectors of sensitive U.S. economic information and technologies, particularly in cyberspace. Non-cyberspace collection methods include targeting of U.S. visitors overseas, especially if the visitors are assessed as having access to sensitive information. It continues to take information warfare to a new level, working to fan anti-U.S. and anti-Western sentiment both within Russia and globally. Russian government officials enter private residences and premises without warrants, and engage in electronic surveillance without appropriate authorization. Applicant's in-laws in Russia create a heightened risk of foreign exploitation, inducement, manipulation, pressure, and coercion. AG ¶¶ 7(a), 7(b), and 7(e) apply.

I have considered all of the mitigating conditions under AG ¶ 8 and considered the following relevant:

> (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 United States;
>
> (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; and
>
> (c) contact or communication with foreign citizens is so casual and infrequent that there is little likelihood that it could create a risk for foreign influence or exploitation.

Applicant's parents-in-law and brother-in-law are Russian citizens residing in Russia. Accordingly, AG ¶ 8(a) is not established for the reasons set out in the above discussion of AG ¶¶ 7(a), 7(b), and 7(e). Applicant's wife maintains regular contact with her family in Russia. She also travels to Russia once yearly to visit them. AG ¶ 8(c) is not established.

Applicant is a native-born U.S. citizen residing in the United States. He served honorably in the U.S. military from 1990 to 1994. His wife became a naturalized U.S. citizen in 2014 and renounced her Russian citizenship in 2016. Their children are native-born U.S. citizens. Though Applicant received $90,000 in 2013 from the sale of his mother-in-law's condominium in Russia, neither he nor his wife have received or expect to receive any additional money from anyone in Russia. Applicant has substantial financial interests in the United States and neither he nor his wife have any such interests in Russia. He has complied with security requirements and reported his foreign travels and receipt of money from his mother-in-law to his FSO. These are all

factors that weigh in Applicant's favor. However, his ties to his family in Russia through his wife are also as strong. As such, Applicant has not met his burden of demonstrating that he would resolve any conflict of interest in favor of the U.S. interest. AG ¶ 8(b) is not established.

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(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 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 have incorporated my comments under Guidelines E, M, and B in my whole-person analysis.

I assessed Applicant's credibility at the hearing. He has not taken responsibility for mischarging a government contract for time spent viewing pornographic material at work. As such, the record evidence leaves me with questions and doubts as to Applicant's eligibility and suitability for a security clearance. I conclude Applicant did not mitigate the personal conduct, use of information technology, and foreign influence 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:	AGAINST APPLICANT
Subparagraphs 1.a - 1.b:	Against Applicant
Paragraph 2, Guideline M:	AGAINST APPLICANT
Subparagraph 2.a:	Against Applicant

Paragraph 3, Guideline B:	AGAINST APPLICANT
Subparagraphs 3.a - 3.c:	Against APPLICANT

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's eligibility for a security clearance. Eligibility for access to classified information is denied.

_____
Candace Le'i Garcia
Administrative Judge