



**DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS**



In the matter of:

Applicant for Security Clearance

)
)
)
)
)

ISCR Case No. 16-01456

Appearances

For Government: Caroline E. Heintzelman, Esq., Department Counsel
For Applicant: *Pro se*

11/14/2017

Decision

HARVEY, Mark, Administrative Judge:

Applicant's family connections to in-laws in the People's Republic of China are close and continuing. The People's Republic of China aggressively seeks classified and protected information from the United States. Foreign influence security concerns are not mitigated. Eligibility for access to classified information is denied.

Statement of the Case

On March 11, 2015, Applicant signed his Questionnaire for National Security Positions (SF 86) or security clearance application (SCA). Government Exhibit (GE) 1. On October 15, 2016, the Department of Defense (DOD) Consolidated Adjudications Facility (CAF) issued a statement of reasons (SOR) to him, alleging security concerns under Guideline B (foreign influence). Hearing Exhibit (HE) 2. The action was taken under Executive Order 10865, *Safeguarding Classified Information within Industry* (February 20, 1990), as amended; DOD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the adjudicative guidelines (AG), which became effective on September 1, 2006 (Sept. 1, 2006 AGs).

On November 8, 2016, Applicant provided a response to the SOR, and he requested a hearing. HE 3. On December 13, 2016, Department Counsel was ready to proceed. On July 5, 2017, the case was assigned to me. On July 5, 2017, the Defense

Office of Hearings and Appeals (DOHA) issued a notice of hearing, setting the hearing for July 11, 2017. HE 1. Applicant's hearing was held as scheduled. Applicant waived his right to 15 days of notice of the date, time, and location of the hearing. Tr. 13-14.

During the hearing, Department Counsel offered two exhibits; Applicant offered two exhibits; there were no objections; and all proffered exhibits were admitted into evidence. Tr. 16-18; GE 1-2; Applicant Exhibits (AE) A-B. On July 19, 2017, DOHA received a copy of the transcript of the hearing.

While this case was pending a decision, the Director of National Intelligence (DNI) issued Security Executive Agent Directive 4, establishing in Appendix A the *National Security Adjudicative Guidelines for Determining Eligibility for Access to Classified Information or Eligibility to Hold a Sensitive Position* (AGs), which he made applicable to all covered individuals who require initial or continued eligibility for access to classified information or eligibility to hold a sensitive position. The new AGs supersede the Sept. 1, 2006 AGs and are effective "for all covered individuals" on or after June 8, 2017. I have evaluated Applicant's security clearance eligibility under the new AGs.¹

Procedural Rulings

Department Counsel requested administrative notice (AN) of facts concerning China. HE 4. The request listed supporting documents to show detail and context for those facts. Department Counsel's AN request is quoted at pages 4-7 *infra*, with footnotes in the original omitted and minor grammatical changes. AG ¶ 6, Foreign Influence, provides, "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." A risk assessment in this case necessitates administrative notice of facts concerning China.

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 at ISCR proceedings is accorded to facts that are either well known or from government reports. See Stein, ADMINISTRATIVE LAW, Section 25.01 (Bender & Co. 2006) (listing fifteen types of facts for administrative notice).

¹ Application of the AGs that were in effect as of the issuance of the SOR would not change my decision in this case. The new AGs are available at http://ogc.osd.mil/doha/SEAD4_20170608.pdf.

Findings of Fact²

The SOR alleges in ¶¶ 1.a and 1.b that Applicant's mother-in-law and sister-in-law are citizens and residents of the People's Republic of China. Applicant admitted both of the SOR allegations, and he provided extenuating and mitigating information. His admissions are incorporated herein as findings of fact. After a complete and thorough review of the evidence of record, I make the following findings of fact.

Applicant is a 31-year-old scientist employed by a defense contractor. Tr. 6. In 2004, he graduated from high school, and in 2008, he received a bachelor's degree in engineering physics. Tr. 6-7. In 2010, he earned a master's degree, and in 2014, he received a Ph.D. degree in physics. Tr. 7. In 2007, he married, and his two children are ages five and two. Tr. 7-8, 26.

From May 2005 to July 2005, Applicant studied in China when he was an undergraduate. Tr. 27-28. He met his future wife while he was in China. Tr. 28. In 2007, shortly before they married, she emigrated from China to the United States. Tr. 28. Applicant's spouse was born in China, and she is now a naturalized U.S. citizen. Tr. 22; AE A at 10-11. China does not recognize dual citizenship, and Applicant's spouse is solely a citizen of the United States. GE 2. Applicant traveled to China in 2005, 2007, and 2009. Tr. 29. His spouse traveled to China in 2009, 2012, and two additional times. Tr. 29. Her most recent visit to China was in February 2017. Tr. 30.

Applicant's father-in-law passed away in 2012. Tr. 28-29. His mother-in-law is a 62-year-old citizen and resident of China, and she was a clerk or accountant for her Chinese county. Tr. 20-21. She retired from this position in 2004. Tr. 21. She receives a government pension. Tr. 33, 35. She traveled to the United States in 2011, 2012, and 2014. Tr. 21, 30. Applicant has intermediate skills in the Chinese language, and he communicates with her using email about family matters. Tr. 21. She is aware that Applicant has a Ph.D. and is employed as a scientist. Tr. 21. He does not discuss other details of his employment with her. Tr. 21. He communicates with her about twice a month, and his spouse communicates with her a little more frequently than Applicant communicates with her. Tr. 31, 36. Applicant made some gifts to his mother-in-law totaling about \$1,200. Tr. 32-33.

Applicant's sister-in-law is a 22-year-old citizen and resident of China, and she is studying for a master's degree in computer science at a university in China. Tr. 22. She is attending school on a government scholarship. Tr. 36. She traveled to the United States in 2013. Tr. 22; AE A at 4. She is aware that Applicant has a Ph.D. and is employed as a scientist. Tr. 23. He does not discuss other details of his employment with her. Tr. 23. He communicates with her using email. Tr. 23. When Applicant's in-laws traveled to the United States, they stayed with Applicant. Tr. 30. He communicates with his sister-in-law about twice a month, and he does not know how often his spouse communicates with her. Tr. 31. Applicant made gifts to his sister-in-law totaling about

² To protect Applicant and his family's privacy, the facts in this decision do not specifically describe employment, names of witnesses, and names of other groups or locations. The cited sources contain more specific information.

\$300. Tr. 32. In 2011, Applicant's sister-in-law applied to move to the United States. Tr. 33; AE A at 10-11.

Applicant stated that his in-laws in China do not have and have never had high-level Chinese Government positions. Tr. 38. He believes his in-laws would not place him in a compromising position. Tr. 38. In the event of a conflict of interest, he would choose the interests of the United States over China. Tr. 38.

Character Evidence

Applicant's supervisor for two years described him as demonstrating exceptional technical creativity and making outstanding contributions to the government. Tr. 34; AE B. He is dedicated and diligent. AE B. His personal conduct is exemplary, and his supervisor recommends approval of his security clearance. AE B.

China

The National Counterintelligence Executive has identified China and Russia as the most aggressive collectors of U.S. economic information and technology. "China's intelligence services, as well as private companies and other entities, frequently seek to exploit Chinese citizens or persons with family ties to China who can use their insider access to corporate networks to steal secrets using removable media devices or e-mail."

In assessing the military and security developments in China, the U.S. Department of Defense has reported that:

"Chinese actors are the world's most active and persistent perpetrators of economic espionage. Chinese attempts to collect U.S. technological and economic information will continue at a high level and will represent a growing and persistent threat to U.S. economic security. The nature of the cyber threat will evolve with continuing technological advances in the global information environment."

"In the long term, Chinese leaders are focused on developing the capabilities they deem necessary to deter or defeat adversary power projection and counter third-part[ies] including U.S.-intervention during a crisis or conflict. China's military modernization is producing capabilities that have the potential to reduce core U.S. military technological advantages."

"China very likely uses its intelligence services and employs other illicit approaches that violate U.S. laws and export controls to obtain key national security and export-restricted technologies, controlled equipment, and other materials unobtainable through other means."

"In 2015, numerous computer systems around the world, including those owned by the U.S. Government, continued to be targeted for intrusions, some of which appear

to be attributable directly to China's Government and military. These and past intrusions were focused on accessing networks and exfiltrating information."

"China is using its cyber capabilities to support intelligence collection against the U.S. diplomatic, economic, and defense industrial base sectors that support U.S. national defense programs. The information targeted could potentially be used to benefit China's defense industry, high-technology industries, and provide [China] insights into U.S. leadership perspectives on key China issues. Additionally, targeted information could inform Chinese military planners' work to build a picture of U.S. defense networks, logistics, and related military capabilities that could be exploited during a crisis."

China uses "State-sponsored industrial and technical espionage to increase the level of technologies and expertise available to support military research, development, and acquisition."

The organizational network of China's military-industrial complex is such that the People's Liberation Army (PLA) is able "to access sensitive and dual-use technologies or knowledgeable experts under the guise of civilian research and development."

As recently as March 2016, for instance, a Chinese national pleaded guilty to participating in a conspiracy, between approximately October 2008 through March 2014, to hack into the computer networks of major U.S. defense contractors, steal sensitive military-including data relating to military aircraft that are indispensable in keeping our military personnel safe--and export-controlled data, and send the stolen data to China.

China has in place "a long-term, comprehensive military modernization program designed to improve its armed forces' capacity to fight short-duration, high-intensity regional conflicts" and, "as China's global footprint and international interests grow, its military modernization program has become progressively more focused on investments for a range of missions beyond China's periphery"

There are also numerous examples of individuals who have been convicted of conspiring to violate federal export control laws by illegally exporting defense equipment to China, of which only the most recent is cited here. Most recently, in June 2016, a California resident was convicted in Federal District Court of conspiring to illegally export fighter jet engines and unmanned aerial vehicles (drones) and related technical data to China, in violation of the Arms Export Control Act.

In assessing the national security implications of the bilateral trade and economic relationship between the U.S. and China, the U.S.-China Economic and Security Review Commission has reported:

"Since at least the mid-2000s, the Chinese government has conducted large-scale cyber espionage against the United States. China has compromised a range of U.S. networks, including those of DoD, defense contractors, and private enterprises."

“China’s material incentives for continuing this activity are immense and unlikely to be altered by small-scale U.S. actions.”

“China’s progress modernizing its defense industry is due in large part to China’s substantial and sustained investment in defense research and development (R&D). China’s large-scale, state-sponsored theft of intellectual property and proprietary information also has allowed China to fill knowledge gaps in its domestic defense and commercial R&D.”

Since the 1990s, China “has promoted ‘civil-military integration’ to facilitate the transfer of commercial technologies for military use. As part of this effort, China has encouraged civilian enterprises to participate in military R&D and production, sponsored research into dual-use science and technology, and developed common military and civilian technical standards.”

“With the emergence of a more modern and able domestic defense industrial base, China is gradually shifting its focus from purchasing complete foreign systems to procuring foreign military and dual-use subsystems and components via open sources, trade, and traditional and nontraditional espionage. Among China’s most effective methods used to acquire sensitive U.S. technology are cyber espionage; witting and unwitting collection by Chinese students, scholars, and scientists; joint ventures; and foreign cooperation.”

With respect to human rights concerns observed in China in 2015, the U.S. Department of State reported:

“The People’s Republic of China (PRC) is an authoritarian state in which the Chinese Communist Party (CCP) is the paramount authority. CCP members hold almost all top government and security apparatus positions.”

“Repression and coercion markedly increased during the year, particularly against organizations and individuals involved in civil and political rights advocacy, and public interest and ethnic minority issues,” and against lawyers and law firms that took on sensitive cases.

Human rights concerns that were observed during 2015 also included: extralegal measures to prevent public expression of critical opinions; repression of speech, religion, association, assembly and movement for certain minorities; extrajudicial killings; enforced disappearance and incommunicado detention, including prolonged detentions at unofficial holding facilities (“black jails”); torture and coerced confessions of prisoners; detention and harassment of individuals who sought to peacefully exercise their rights under the law; a lack of due process in judicial proceedings; searches of premises without warrants; monitoring of communications (including telephone conversations, facsimile transmissions, e-mail, text messaging, and Internet communications); opening of domestic and international mail; failure to respect freedom of speech and the press; severe restrictions on peaceful assembly, as well as severe

restrictions on citizens' freedom of association. Additionally, citizens lacked the right to change their government and had limited forms of redress against the government.

The U.S. Department of State warns visitors to China that they may be placed under surveillance. "Hotel rooms (including meeting rooms), offices, cars, taxis, telephones, Internet usage, and fax machines may be monitored onsite or remotely, and personal possessions in hotel rooms, including computers, may be searched" without knowledge or consent.

Policies

The U.S. Supreme Court has recognized the substantial discretion of the Executive Branch in regulating access to information pertaining to national security emphasizing, "no one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988). As Commander in Chief, the President has the authority to control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to have access to such information." *Id.* at 527. The President has authorized the Secretary of Defense or his designee to grant applicant's eligibility for access to classified information "only upon a finding that it is clearly consistent with the national interest to do so." Exec. Or. 10865, *Safeguarding Classified Information within Industry* § 2 (Feb. 20, 1960), as amended.

Eligibility for a security clearance is predicated upon the applicant meeting the criteria contained in the adjudicative guidelines. These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, these guidelines are applied in conjunction with an evaluation of the whole person. An administrative judge's overarching adjudicative goal is a fair, impartial, and commonsense decision. An administrative judge must consider all available, reliable information about the person, past and present, favorable and unfavorable.

The Government reposes a high degree of trust and confidence in persons with access to classified information. This relationship transcends normal duty hours and endures throughout off-duty hours. 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 about potential, rather than actual, risk of compromise of classified information. Clearance decisions must be "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." See Exec. Or. 10865 § 7. See also Executive Order 12968 (Aug. 2, 1995), § 3.1. Thus, nothing in this Decision should be construed to suggest that I have based this decision, in whole or in part, on any express or implied determination about applicant's allegiance, loyalty, or patriotism. It is merely an indication the applicant has not met the strict guidelines the President and the Secretary of Defense have established for issuing a clearance.

Initially, the Government must establish, by substantial evidence, conditions in the personal or professional history of the applicant that may disqualify the applicant from being eligible for access to classified information. The Government has the burden

of establishing controverted facts alleged in the SOR. See *Egan*, 484 U.S. at 531. “Substantial evidence” is “more than a scintilla but less than a preponderance.” See *v. Washington Metro. Area Transit Auth.*, 36 F.3d 375, 380 (4th Cir. 1994). The guidelines presume a nexus or rational connection between proven conduct under any of the criteria listed therein and an applicant’s security suitability. See ISCR Case No. 95-0611 at 2 (App. Bd. May 2, 1996).

Once the Government establishes a disqualifying condition by substantial evidence, the burden shifts to the applicant to rebut, explain, extenuate, or mitigate the facts. Directive ¶ E3.1.15. An applicant “has the ultimate burden of demonstrating that it is clearly consistent with the national interest to grant or continue his or her security clearance.” ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002). The burden of disproving a mitigating condition never shifts to the Government. See ISCR Case No. 02-31154 at 5 (App. Bd. Sep. 22, 2005). “[S]ecurity clearance determinations should err, if they must, on the side of denials.” *Egan*, 484 U.S. at 531; see AG ¶ 2(b).

Analysis

Foreign Influence

AG ¶ 6 explains the security concern about foreign influence 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 three conditions that could raise a security 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;

(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.

Applicant's spouse was born in China. In 2007, she immigrated to the United States, and she was naturalized as a U.S. citizen. Her mother and sister are citizens and residents of China. He has frequent³ contact with his mother-in-law and sister-in-law, and his spouse has frequent contact with her mother.

Applicant lives with and is close to his spouse. His spouse has relatives living in China. There is a rebuttable presumption that a person has ties of affection for, or obligation to, their immediate family members. See *generally* ISCR Case No. 01-03120, 2002 DOHA LEXIS 94 at *8 (App. Bd. Feb. 20, 2002). "[A]s a matter of common sense and human experience, there is [also] a rebuttable presumption that a person has ties of affection for, or obligation to, the immediate family members of the person's spouse." ISCR Case No. 07-17673 at 3 (App. Bd. Apr. 2, 2009) (citing ISCR Case No. 01-03120 at 4 (App. Bd. Feb. 20, 2002)). This concept is the basis of AG ¶ 7(e). Indirect influence from a spouse's relatives living in China could result in a security concern. See ISCR Case No. 09-05812 at 2 (App. Bd. Dec. 1, 2011) (finding "presence in India of close family members, viewed in light of that country's troubles with terrorism and its human rights abuses, and his sharing living quarters with a person (his spouse) having foreign family contacts, establish the 'heightened risk'" in AG ¶¶ 7(b) and 7(e)).

Applicant and his spouse's relationships with residents of China create a concern about Applicant's "obligation to protect sensitive information or technology" and his desire to help relatives living in China. For example, if intelligence officials, or other entities in China, wanted to expose Applicant to coercion, they could exert pressure on his spouse's relatives living in China. Applicant would then be subject to coercion through his connections to China and classified information could potentially be compromised.

Applicant and his spouse's close family ties with her family living in China, are not, as a matter of law, disqualifying under Guideline B. However, if an applicant or his spouse has a close relationship with even one relative, living in a foreign country, this factor alone is sufficient to create the potential for foreign influence and could potentially result in the compromise of classified information. See ISCR Case No. 03-02382 at 5 (App. Bd. Feb. 15, 2006); ISCR Case No. 99-0424 (App. Bd. Feb. 8, 2001).

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 or inducement. 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 collection operations against the United States. The relationship of China with the United States, places a significant, but not an

³ See ISCR Case No. 09-03114 at 2-3 (App. Bd. Oct. 22, 2010) (contact once a month is considered to be "frequent" under AG ¶¶ 7 and 8).

insurmountable burden of persuasion on Applicant to demonstrate that his and his spouse's relationships with family members living in China do not pose a security risk. Applicant should not be placed into a position where he might be forced to choose between loyalty to the United States and a desire to assist relatives in China.

Guideline B is not limited to countries hostile to the United States. "The United States has a compelling interest in protecting and safeguarding classified information from any person, organization, or country that is not authorized to have access to it, regardless of whether that person, organization, or country has interests inimical to those of the United States." ISCR Case No. 02-11570 at 5 (App. Bd. May 19, 2004). Furthermore, friendly nations can have profound disagreements with the United States over matters they view as important to their vital interests or national security. Finally, we know friendly nations have engaged in espionage against the United States, especially in the economic, scientific, and technical fields. See ISCR Case No. 00-0317, 2002 DOHA LEXIS 83 at **15-16 (App. Bd. Mar. 29, 2002).

While there is no evidence that intelligence operatives or terrorists from China seek or have sought classified or economic information from or through Applicant, his spouse, or their relatives living in China, nevertheless, it is not possible to rule out such a possibility in the future. Applicant and his spouse's relationships with family members living in China create a potential conflict of interest because these relationships are sufficiently close to raise a security concern about his desire to assist her relatives in China by providing sensitive or classified information. Department Counsel produced substantial evidence of Applicant and his spouse's relationships with her family living in China. Department Counsel has raised the issue of potential foreign pressure or attempted exploitation, and further inquiry is necessary about potential application of any mitigating conditions.

AG ¶ 8 lists six conditions that could mitigate foreign influence security 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.;
- (b) there is no conflict of interest, either because the individual's sense of loyalty or obligation to the foreign person, group, government, or country is so minimal, or the individual has such deep and longstanding relationships and loyalties in the U.S., that the individual can be expected to resolve any conflict of interest in favor of the U.S. interest;
- (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;

(d) the foreign contacts and activities are on U.S. Government business or are approved by the cognizant security authority;

(e) the individual has promptly complied with existing agency requirements regarding the reporting of contacts, requests, or threats from persons, groups, or organizations from a foreign country; and

(f) the value or routine nature of the foreign business, financial, or property interests is such that they are unlikely to result in a conflict and could not be used effectively to influence, manipulate, or pressure the individual.

The Appeal Board concisely explained Applicant's responsibility for proving the applicability of mitigating conditions as follows:

Once a concern arises regarding an Applicant's security clearance eligibility, there is a strong presumption against the grant or maintenance of a security clearance. See *Dorfmont v. Brown*, 913 F. 2d 1399, 1401 (9th Cir. 1990), *cert. denied*, 499 U.S. 905 (1991). After the Government presents evidence raising security concerns, the burden shifts to the applicant to rebut or mitigate those concerns. See Directive ¶ E3.1.15. The standard applicable in security clearance decisions is that articulated in *Egan, supra*. "Any doubt concerning personnel being considered for access to classified information will be resolved in favor of the national security." Directive, Enclosure 2 ¶ 2(b).

ISCR Case No. 10-04641 at 4 (App. Bd. Sept. 24, 2013).

AG ¶¶ 8(a) and 8(c) have limited applicability. Applicant and his spouse have frequent contacts with her relatives living in China. Their contacts and communications are casual and family related; however, Applicant's in-laws in China are aware that he is a scientist with a Ph.D. Moreover, they communicate using email, and Chinese intelligence officials are known to monitor email. Loyalty to, support for, and connections to family are positive character traits. However, for security clearance purposes, those same relationships and Applicant's specialized education and background negate the possibility of full mitigation under AG ¶¶ 8(a) and 8(c). Applicant failed to fully meet his burden of showing there is little likelihood that his relationships with relatives in China could create a risk for foreign influence or exploitation.

AG ¶ 8(b) partially applies. A key factor in the AG ¶ 8(b) analysis is Applicant's "deep and longstanding relationships and loyalties in the U.S." Applicant has significant connections to the United States. Applicant, his spouse, and his two children are citizens and residents of the United States. China does not recognize dual citizenship, and Applicant's spouse is solely a citizen of the United States. When Applicant volunteered to assist the U.S. Government as a contractor, he manifested his patriotism, loyalty, and fidelity to the United States over all other countries.

Applicant's relationship with the United States must be weighed against the potential conflict of interest created by his relationships with family living in China. There is no evidence, however, that terrorists, criminals, the Chinese Government, or those conducting espionage have approached or threatened Applicant, his spouse, or their relatives living in China to coerce Applicant for classified or sensitive information.⁴ As such, there is a reduced possibility that Applicant, his spouse, or her relatives living in China would be specifically selected as targets for improper coercion or exploitation.

While the U.S. Government does not have any burden to prove the presence of such evidence, if such record evidence were present, Applicant would have a heavier evidentiary burden to mitigate foreign influence security concerns. It is important to be mindful of the United States' sizable financial and diplomatic investment in China. Applicant's spouse's relatives living in China could become potential targets because of Applicant's support for the United States, and Applicant's potential access to classified information could theoretically add some risk to them from intelligence elements in China.

AG ¶¶ 8(d), 8(e), and 8(f) do not apply. The U.S. Government has not encouraged Applicant's involvement with anyone living in China. Applicant is not required to report his contacts with citizens or residents of China. There is insufficient information about Applicant's assets in the United States to mitigate security concerns.

In sum, Applicant and his spouse's connections to her relatives living in China are significant. She is sufficiently close to family in China to raise a security concern. Her mother and sister are citizens and residents of China. Applicant has frequent contact with his mother-in-law and sister-in-law, and his spouse has frequent contact with her mother. His mother-in-law and sister-in-law have visited Applicant in the United States. His mother-in-law and sister-in-law received funds from Applicant, and they receive funds from the Chinese government (pension and scholarship funds). Applicant traveled to China in 2005, 2007, and 2009. His spouse traveled to China four times after emigrating from China to the United States. Her most recent visit to China was in February 2017. Applicant has significant connections to the United States; however, they are not sufficient to overcome his and his spouse's connections to China. Foreign influence security concerns are not mitigated.

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 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

⁴ There would be little reason for U.S. enemies to seek classified information from an applicant before that applicant has access to such information or before they learn of such access.

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), "[t]he 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. My comments under Guideline B are incorporated in my whole-person analysis. Some of the factors in AG ¶ 2(d) were addressed under that guideline but some warrant additional comment.

Applicant is a 31-year-old scientist employed by a defense contractor. In 2004, he graduated from high school, and in 2008, he received a bachelor's degree in engineering physics. In 2010, he earned a master's degree, and in 2014, he received a Ph.D. degree in physics. In 2007, he married, and his two children are ages five and two. Applicant's supervisor for two years described him as demonstrating exceptional technical creativity and making outstanding contributions to the government. He is dedicated and diligent. His personal conduct is exemplary, and his supervisor recommends approval of his security clearance.

Applicant has significant connections to China. Applicant's spouse was born in China. In 2007, she emigrated from China to the United States, and she was naturalized as a U.S. citizen. Her mother and sister are citizens and residents of China. Applicant has frequent contact with his mother-in-law and sister-in-law. Applicant and his spouse have visited China since 2007 several times, and her relatives from China have visited Applicant and his family in the United States. Applicant has provided financial gifts to his mother-in-law and sister-in-law. Applicant's mother-in-law and sister-in-law know he is a scientist with a Ph.D. They communicate with him using email, and Chinese intelligence monitors email.

In ISCR Case No. 15-00528 at 3-4 (App. Bd. Mar. 13, 2017) the Appeal Board considered a Guideline B case involving a U.S. citizen with family members in China and commented:

In Foreign Influence cases, the nature of the foreign government involved and the intelligence gathering history of that government are among the important considerations that provide context for the other record evidence and must be brought to bear on the Judge's ultimate conclusions in the case. The country's human rights record is another important consideration. See, e.g., ISCR Case No. 05-03250 at 4-5 (App. Bd. Apr. 6, 2007); ISCR Case No. 04-11463 at 4 (App. Bd. Aug. 4, 2006). There is a rational connection between an applicant's family ties in a country whose interests are adverse to the United States and the risk that the applicant might fail to protect and safeguard classified information. See, e.g., ISCR Case No. 10-07436 at 3, n. 4 (App. Bd. Oct. 19, 2011).

We note record evidence and the Judge's findings of the following: Applicant's parents reside in China; Applicant communicates with them frequently; Applicant has visited them or they her on a regular basis; Applicant's parents are aware of the location and general nature of her work; China practices espionage against the U.S.; and China has used its cyber-espionage capability to compromise DoD and contractor computer systems. This evidence supports the Judge's conclusion that Applicant's parents could become a means through which Applicant could come to the attention of Chinese intelligence personnel and be subjected to coercion or pressure.

There are some factual differences between Applicant's case, and ISCR Case No. 15-00528 (App. Bd. Mar. 13, 2017); however, the issues of security concern in that case and Applicant's case are similar. See *e.g.*, ISCR Case No. 15-00042 (App. Bd. July 6, 2016) (denial of security clearance due to connections to China affirmed); ISCR Case No. 14-03200 (App. Bd. July 16, 2015) (same); ISCR Case No. 12-04780 at 3 (App. Bd. Nov. 13, 2013) (stating "The PRC's history of conducting espionage against the United States puts a heavy burden of proof on Applicant that he was unable to meet because of his ties to his relatives who are PRC citizens and residents.").

I have carefully applied the law, as set forth in *Egan*, Exec. Or. 10865, the Directive, and the AGs, to the facts and circumstances in the context of the whole person. I conclude that foreign influence security concerns are not mitigated. It is not clearly consistent with the interests of national security to grant Applicant security clearance eligibility.

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:	AGAINST APPLICANT
---------------------------	-------------------

Subparagraphs 1.a and 1.b:	Against Applicant
----------------------------	-------------------

Conclusion

In light of all of the circumstances presented by the record in this case, it is not clearly consistent with national security to grant Applicant eligibility for a security clearance. Eligibility for access to classified information is denied.

Mark Harvey
Administrative Judge