



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



In the matter of:)
)
) ISCR Case No. 16-02130
)
Applicant for Security Clearance)

Appearances

For Government: Benjamin R. Dorsey, Esq., Department Counsel
For Applicant: *Pro se*

10/30/2017

Decision

KILMARTIN, Robert J., Administrative Judge:

Applicant has mitigated foreign influence security concerns. Eligibility for access to classified information is granted.

Statement of the Case

On September 30, 2016, the Department of Defense (DOD) issued a Statement of Reasons (SOR) to Applicant detailing security concerns under Guideline C (foreign preference) and Guideline B (foreign influence). The action was taken under Executive Order (EO) 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) implemented by the DOD on September 1, 2006.

On December 10, 2016, the Director of National Intelligence issued Security Executive Agent Directive (SEAD) 4, revising the 2006 AGs. The revised AG apply to all adjudicative decisions issued on or after June 8, 2017. I have based my decision on the newly effective AG.

Applicant answered the SOR on October 27, 2016, and elected to have his case decided on the written record in lieu of a hearing. Department Counsel submitted the Government's file of relevant material (FORM) on December 21, 2016. Applicant received the FORM on January 3, 2017, and had 30 days to submit material in refutation, extenuation, or mitigation. Applicant responded on January 26, 2017, by providing a two-page-typed statement plus attachments including copies of his U.S. and Canadian passports and an e-mail dated January 23, 2017. This response was marked as Applicant's Exhibit (AE) A and it was admitted into evidence without objection. The Government's documents, identified as Items 1 through 6, were also admitted into evidence without objection. The case was assigned to me on October 1, 2017.

Request for Administrative Notice

Department Counsel submitted a written request that I take administrative notice of certain facts about China or the Peoples Republic of China (PRC). Item 6. The request and the attached source documents were not admitted into evidence but were included in the record as Hearing Exhibit (HE) I.

The request listed supporting documents to show detail and context for those facts. AG ¶ 6, Foreign Influence, provides, "Adjudication under this Guideline can and should consider the identity of the foreign country in which the foreign contact or financial interest is located, including, but not limited to, such considerations as whether the foreign country is known to target United States citizens to obtain protected information and/or is associated with a risk of terrorism." A risk assessment in this case necessitates administrative notice of facts concerning the PRC.

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).

Applicant did not object, and I have taken administrative notice of the facts contained in the HE I source documents, and incorporated them by reference. The facts are summarized in the written request and will not be repeated in this decision. However, of particular note, are the following salient facts gleaned from HE 1.

PEOPLE'S REPUBLIC OF 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 DOD 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. Chinese leaders are focused on developing the capabilities they deem necessary to deter or defeat adversary power projection and counter third-party 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.

Further, the DOD found that 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. 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. 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. 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.

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.

With respect to human rights concerns observed in China, 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 have markedly increased recently, particularly against organizations and

individuals involved in civil and political rights advocacy, and public interest and ethnic minority issues, and against law firms that took on sensitive cases.

Human rights concerns that were observed included: extralegal measures to prevent public expression of critical opinions; repression of free speech, religion, association, assembly and movement for certain minorities; extrajudicial killings; enforced disappearance and incommunicado detention, including prolonged detentions in "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; searches of premises without warrants; monitoring of communications; opening of domestic and international mail; as well as severe restrictions on citizens' freedom of association and free speech.

Findings of Fact¹

Applicant is 63 years old. He was born in PRC and moved to Canada in 1987 to attend graduate school. He obtained Canadian citizenship in 1993. He reports obtaining a doctorate degree in chemistry from a Chinese University in 1994, and a master's degree in information technology from a Canadian University in 1997. Applicant came to the United States in January 1998 for employment. He was naturalized on March 5, 2010 and he has been employed as a senior-software-engineer for a federal contractor since April 2014. He is applying for a security clearance for the first time.

Applicant submitted a Questionnaire for National Security Positions (SCA) on June 10, 2014.² In section 18 of his SCA, he disclosed his siblings, including two adopted brothers, and an adopted sister, who are citizens and residents of the PRC. All three siblings work in the banking industry in the PRC and have never had any affiliation with the PRC government. Applicant last had in-person contacts with his siblings at his mother's funeral in the PRC in March 2014. His father had previously passed away in 2010. He has telephonic contact with brother one only once every few months (seven phone calls during all of 2015 and 2016), and with brother two quarterly. He has contact with his sister annually. Applicant has no other contact, via e-mail or otherwise, with his siblings. He also disclosed his foreign travel in his SCA including trips to the PRC in 2007, 2009, 2010, 2012, 2013, and 2014. He traveled to Canada 12 times after becoming a U.S. citizen, using his Canadian passport to enter Canada each time.

Applicant has been married since 1983 and he reports no military service. Applicant has worked in the United States for almost 20 years, with no issues. He has no contact with foreign governments and he has no sympathy, preference for, or alliance with foreign nationals. Applicant admitted all of the allegations in the SOR under Guidelines B and C. He disclosed his possession of a Canadian passport in his SCA. He used it to come to the United States and renewed it in September 2015, with an

¹ Unless otherwise stated, the basis for these findings of fact is Applicant's Questionnaire for National Security Positions (SCA) dated June 10, 2014 (Item 3) and the summary of his clearance interview by a clearance investigator on March 16, 2015. (Item 4)

² Item 3.

expiration date in September 2020. His intent was to only use this passport for travel to Canada. In his October 2016 Answer to the SOR, Applicant stated his willingness to surrender this passport, and described his previous efforts to do so. He has now produced evidence in the form of a January 23, 2017 e-mail from his facilities security officer, attached to his Response to the FORM, showing that he did surrender the Canadian passport in January 2017.

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(c), the entire process is a conscientious scrutiny of a number of variables known as the "whole-person concept." The administrative judge must consider all available, reliable information about the person, past and present, favorable and unfavorable, in making a decision.

The protection of the national security is the paramount consideration. AG ¶ 2(b) requires that "[a]ny doubt concerning personnel being considered for 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 EO 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 EO 12968, Section 3.1(b) (listing multiple prerequisites for access to classified or sensitive information).

Analysis

Guideline C, Foreign Preference

The security concern for foreign preference is set out in AG ¶ 9, as follows:

The Concern. When an individual acts in such a way as to indicate a preference for a foreign country over the United States, then he or she may provide information or make decisions that are harmful to the interests of the United States. Foreign involvement raises concerns about an individual's judgment, reliability, and trustworthiness when it is in conflict with U.S. national interests or when the individual acts to conceal it. *By itself*, the fact that a U.S. citizen is also a citizen of another country is not disqualifying without an objective showing of such conflict or attempt at concealment. The same is true for a U.S. citizen's exercise of any right or privilege of foreign citizenship and any action to acquire or obtain recognition of a foreign citizenship.

Conditions that could raise a security concern and may be disqualifying include:

- (a) applying for and/or acquiring citizenship in any other country;
- (b) failure to report, or fully disclose when required, to an appropriate security official, the possession of a passport or identity card issued by any country other than the United States;
- (c) failure to use a U.S. passport when entering or exiting the U.S.; and
- (d) participation in foreign activities, including but not limited to:

Conditions that could potentially mitigate security concerns include:

- (a) the foreign citizenship is not in conflict with U.S. national security interests;
- (b) dual citizenship is based solely on parental citizenship or birth in a foreign country, and there is no evidence of foreign preference;
- (c) the individual has expressed a willingness to renounce the foreign citizenship that is in conflict with U.S. national security interests;
- (d) the exercise of the rights, privileges, or obligations of foreign

citizenship occurred before the individual became a U.S. citizen;

(e) the exercise of the entitlements or benefits of foreign citizenship do not present a national security concern; and

(f) the foreign preference, if detected, involves a foreign country, entity, or association that poses a low national security risk;

Applicant traveled to Canada roughly 12 times after becoming a U.S. citizen in 2010. He possessed the Canadian passport for convenience sake, to facilitate entry to Canada. He never used the Canadian passport for any other purpose. Canada is not hostile to the United States, and dual-citizenship with Canada, or travel to and from Canada, presents no conflict with U.S. national security interests. In any event, Applicant surrendered the Canadian passport to his FSO in January 2017. He has indicated no continuing allegiance to Canada. The mitigating conditions above at AG ¶ 11 apply. I find that Applicant has expressed no preference for a foreign country over the United States.

Guideline B, Foreign Influence

The security concern for foreign influence is set out in AG ¶ 6:

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 that is 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, such considerations as whether the foreign country is known to target United States citizens to obtain classified or sensitive information or is associated with a risk of terrorism.

The guideline notes several conditions that could raise security concerns under AG ¶ 7. The following are potentially applicable 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;

(c) failure to report or fully disclose, when required, association with a foreign person, group, government, or country; and

(f) substantial business, financial, or property interests in a foreign country, or in any foreign-owned or foreign-operated business that could subject the individual to heightened risk of foreign influence or exploitation or personal conflict of interest.

Applicant's siblings are citizens and residents of the PRC. PRC is continuously engaged in cyber-espionage against the United States, economic espionage, and human rights abuses. Applicant's foreign contacts may create a potential conflict of interest and a heightened risk of foreign exploitation, inducement, manipulation, pressure, and coercion, both directly and through his family members. AG ¶¶ 7(a) and 7(b) have been raised by the evidence.

Conditions that could potentially mitigate foreign influence security concerns are provided under AG ¶ 8. The following are potentially applicable:

(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 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 agency head or designee;

(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.

I considered the totality of Applicant's foreign contacts and interests. 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.³

The distinctions between friendly and unfriendly governments must be made with caution. Relations between nations can shift, sometimes dramatically and unexpectedly. Furthermore, friendly nations can have profound disagreements with the U.S. 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. The nature of a nation's government, its relationship with the U.S., and its human rights record are relevant in assessing whether 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, the country is known to conduct intelligence operations against the U.S., or the foreign country is associated with a risk of terrorism.

Applicant came to the United States in 1998. He became a U.S. citizen in 2010. He is married and has been employed in the U.S. for nearly 20 years. He appears to be a solid citizen. He has longstanding relationships and loyalties here. Although he has siblings in the PRC, which is an authoritarian regime, his contact with them is *de-minimis*. He continues to have only fleeting, occasional contact with his family members in the PRC. There is no indication that they are affiliated with the Chinese government or intelligence services. Applicant is committed to his new life here. AG ¶¶ 8(a), (b), and (c) are applicable to the PRC family members contacts, which are alleged in SOR ¶¶ 2.a. Because Applicant's ties to the PRC are minimal and inconsequential, I find that all foreign influence concerns have been 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 relevant circumstances. The administrative judge should consider the nine adjudicative process factors listed at AG ¶ 2(d):

³ ISCR Case No. 02-11570 at 5 (App. Bd. May 19, 2004).

(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 B and C in my whole-person analysis. Some of the factors in AG ¶ 2(d) were addressed under those guidelines.

Overall, the record evidence leaves me with no questions or doubts as to Applicant's eligibility and suitability for a security clearance. I conclude Applicant has mitigated foreign influence and foreign preference 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 C:	FOR Applicant
Subparagraph 1.a:	For Applicant
Paragraph 2, Guideline B:	For Applicant
Subparagraph a:	For Applicant

Conclusion

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

Robert J. Kilmartin
Administrative Judge