DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
[Redacted]	)	ISCR Case No. 11-12623
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Eric H. Borgstrom, Esq., Department Counsel
For Applicant: David H. Shapiro, Esq.

09/30/2014

_____

Decision

_____

FOREMAN, LeRoy F., Administrative Judge:

This case involves security concerns raised under Guidelines B (Foreign Influence), K (Handling Protected Information), and E (Personal Conduct). Eligibility for access to classified information is granted.

Statement of the Case

Applicant submitted a security clearance application on May 11, 2010. On March 26, 2013, the Department of Defense (DOD) sent him a Statement of Reasons (SOR) alleging security concerns under Guidelines B, K, and E. The DOD acted under Executive Order 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 DOD on September 1, 2006.

Applicant received the SOR on April 4, 2013; answered it on April 22, 2013; and requested a hearing before an administrative judge. Department Counsel sent Applicant an amended SOR on May 15, 2014, which Applicant answered on May 29, 2014. Department Counsel was ready to proceed on June 9, 2014, and the case was

assigned to me on June 10, 2014. On June 13, 2014, the Defense Office of Hearings and Appeals (DOHA) issued a notice of hearing, scheduling the hearing for July 9, 2014. The hearing was postponed at Applicant's request for medical reasons. On August 8, 2014, DOHA issued another notice of hearing, scheduling the hearing for August 27, 2014. I convened the hearing as scheduled. Government Exhibits (GX) 1 through 6 and 8 through 14 were admitted in evidence without objection. Applicant objected to GX 7, and I deferred ruling on the objection. Neither side objected to deferring the decision on admissibility. I have admitted GX 7, for the reasons set out below. Applicant testified, presented the testimony of four witnesses, and submitted Applicant's Exhibits (AX) 1 through 13, which were admitted without objection. DOHA received the transcript (Tr.) on September 8, 2014.

Administrative Notice

Department Counsel requested that I take administrative notice of relevant facts about Israel. The request and supporting documents are attached to the record as Hearing Exhibit (HX) I. Applicant objected to Department Counsel's request on the ground that the materials submitted were one-sided and did not present an objective, balanced view of Israel. I offered Applicant an opportunity to submit a separate request for administrative notice, and he orally requested that I take administrative notice of additional facts related to the relationship between the United States and Israel. (Tr. 41, 296-97.) I took administrative notice as requested by Department Counsel and Applicant. The facts administratively noticed are set out below in my findings of fact.

Evidentiary Ruling

Applicant objected to GX 7 on the ground that it was multi-level hearsay, irrelevant, and "not authoritative." (Tr. 27-31.) I took the objection under advisement and, without objection from either side, deferred ruling on the admissibility of GX 7. (Tr. 33.)

GX 7 is an unclassified extract of a report previously provided to DOD by another government agency (AGA). It was prepared in response to Department Counsel's request for unclassified copies of "any documents or reports concerning [Applicant's] contacts with foreign nationals or intelligence agents or concerning the June 2009 security incident." (GX 14) The "security incident" is described below in my findings of fact.

Directive E3.1.22 entitles applicants to cross-examine a person who has made an adverse statement on a controverted issue, except under certain circumstances not applicable in this case. However, Directive E3.1.20 permits admission of "official records or evidence compiled or created in the regular course of business, other than DoD personnel background reports of investigation (ROI), without an authenticating witness." GX 7 consists of evidence compiled by the AGA in the regular course of business. GX 7 is not covered by the authentication requirement in Directive E3.1.20, because it is not a "DoD" ROI. *See* ISCR Case No. 10-08390 (App. Bd. Mar. 30, 2012) at 4. Furthermore,

using the Federal Rule of Evidence 803(8) as a guide, I conclude that GX 7 is admissible as a public record because it sets out "factual findings from a legally authorized investigation," and "neither the source of information nor other circumstances indicate a lack of trustworthiness." The fact that GX 7 contains multiple levels of hearsay does not preclude its admission, but affects its weight. It is well settled that hearsay evidence may be considered in federal administrative proceedings, including security clearance adjudications. *See* ISCR Case No. 03-06770 at 4 (App. Bd. Sep. 9, 2004). In light of all the above considerations, I have admitted GX 7 over Applicant's objection.

Findings of Fact

In his answer to the SOR as amended, Applicant admitted SOR ¶¶ 1.b-1e. He denied SOR ¶¶ 1.a, 2.a, 2.b, and 3.a-3.c. His admissions in his answer and at the hearing are incorporated in my findings of fact.

Applicant is a 67-year-old project engineering manager employed by a defense contractor since July 1972. (Tr. 163.) He has a bachelor's degree in computer science and a master's degree in computer science occupational research. He has held a security clearance for virtually all his career as a contractor employee.

Applicant's passport reflects that he was born in Israel, but Israel did not exist in 1947, when he was born. He was born in the part of the British mandated territory of Palestine that became Israel in 1948. (Tr. 231.) He came to the United States with his parents when he was four years old, and became a U.S. citizen in January 1958. He married a native-born U.S. citizen in September 1970. He and his wife have four adult children who are native-born U.S. citizens.

Applicant's 33-year-old son attended a university in Israel from 1998 to 2003, obtained an undergraduate degree, returned to the United States for one year, was married to a native-born U.S. citizen in January 2004, and then returned to Israel from 2004 to July 2010, specializing in Talmudic studies. (Tr. 82.) He received a stipend from an Israeli organization while studying in Israel and allowance of $200 per month from his parents. (Tr. 100, 256.) He has not returned to Israel since completing his studies in 2010. (Tr. 92.)

While in Israel, Applicant's son held a student visa that carried a notation "not allowed to work." (AX 8.) His wife joined him in Israel and worked as a bookkeeper in a school for American girls. (Tr.85.) His wife's parents are citizens and residents of the United States. His wife's brother, sister-in-law, and their children are citizens of the United States residing in Israel. His wife's brother and sister-in-law are teachers in a religious school. (Tr. 95-96.)

While Applicant's son was studying in Israel, he and his family received health benefits from the Israeli government but no other benefits. (Tr. 99.) In 2002, he obtained a certificate from the Israeli Ministry of the Interior stating that he was not an Israeli citizen. (AX 9.) He and his wife had two children while residing in Israel, and he

obtained certificates from the Ministry of the Interior stating that his children were not Israeli citizens. (AX 10-11.) He testified at the hearing that he is a citizen of the United States and not a dual citizen. (Tr. 83.) He submitted a copy of the Israeli law regarding his and his children's non-citizen status in Israel. (AX 12.) He is now employed in the United States as a Talmudic researcher and receives a stipend from a U.S. non-profit organization devoted to promoting Talmudic studies. (Tr. 81, 91.)

Two of Applicant's daughters attended an Israeli university for one year, between high school and college. They reside in the United States. One daughter is married to a U.S. citizen. The others are unmarried. (Tr. 74; GX 4 at 3.) 3.)

Applicant's parents were born in Germany and became U.S. citizens. His parents are deceased. His stepmother is a native-born U.S. citizen who resides in the United States. (Tr. 55-56.)

Applicant's brother was born in Israel, immigrated to the United States, became a U.S. citizen, married a native-born U.S. citizen, and then returned to Israel in 1984. When asked why his brother returned to Israel, Applicant testified, "I think he just felt he had to be there." (Tr. 259.) His brother is a certified public accountant employed by a U.S.-based accounting company. (Tr. 180.) Applicant's brother and sister-in-law are dual citizens of Israel and the United States. (Tr. 178.) Applicant's contact with his brother was "very infrequent" until their father became ill and passed away in 2013. They now have contact about every other month about their father's memorial service and Applicant's recent medical problems. (Tr. 179, 263-64.) Applicant's brother has never introduced him to Israeli officials or sought information about his work. (Tr. 180.) Applicant's last conversation with his brother was in June 2014, when his cousin died. (Tr. 262.)

Applicant's three nieces and three nephews (his brother's children) reside in Israel. Two nieces and one nephew are dual citizens of the United States and Israel, and two nephews and one niece are citizens of Israel. Applicant and his wife have minimal contact with their nieces and nephews. (Tr. 66, 181-82.)

One of Applicant's nieces was active in a political party in Israel and then employed by the Israeli government as a transportation coordinator for a senior Israeli official. She is no longer employed by the Israeli government, but she continues to list her former employer as an employment reference. She is now a trip planner for Christian organizations traveling to Israel. She has never introduced Applicant to Israeli officials or sought information about his work. (Tr. 183-84, 267-68.)

Applicant traveled to Israel to visit his family every January from 2004 to 2010, except for 2007, when he could not afford it. (GX 4 at 2.) Starting at some time in 2009, Applicant's employer began requiring employees with security clearances to report personal foreign travel. (GX 11.) The alternate FSO for Applicant's employer submitted an email stating that her records did not contain any foreign travel reports from Applicant. (GX 10 at 2.) Applicant testified that he traveled to Israel in January 2009 to

visit family and participate in a religious event triggered by the birth of a grandson was well known among his colleagues, but he was unaware that there was a requirement to report personal foreign travel in January 2009. (Tr. 207-08.),

Applicant testified that he went to Israel again in January 2010 and he reported it by email in accordance with the new reporting policy. (Tr. 208-10.) He has no explanation for the absence of entries in the FSO's foreign travel records for his trip to Israel in 2010, but the assistant FSO's memorandum suggests that his foreign travel report may have been filed with his supervisor instead of the FSO. (Tr. 257.) He has not traveled abroad for personal or official reasons since 2010, when his son, daughter-in-law, and grandchildren returned to the United States. (Tr. 281.)

In 1974, Applicant was involved in training two Israeli officers on the software for the F-15 aircraft. Following the training, Applicant and his wife invited one of the officers to join them for a Sabbath dinner, worship at their synagogue, and to spend the night in their home. The officer was staying alone in a hotel and unable to cook without breaking the Sabbath. Their conversations during the visit pertained to family and small talk, with no discussion of the training. They had no further contact with the officer. (GX 7 at 5; Tr. 61-63; 243-46.) Applicant did not report his non-official contact with the officer. Department Counsel submitted no evidence showing a duty to report a single social or religious contact with the Israeli officer under the circumstances of this case. The incident is not alleged in the SOR.

In 1982-83, Applicant was involved with training Israeli officers on software used on the F-15 aircraft. The training included use of the "threat table" contained in the software, which was the most sensitive component because it contained "signature" and "recognition" data. (GX 7 at 3-4.) Applicant testified that he and his coworkers told the Israelis how the software worked, but they were not allowed to disclose any threat information. (Tr. 237.)

According to AGA investigative report, Applicant was removed from a project in May 2005, after working on it for three years. The report states that his removal resulted in performance counseling from his supervisor and resentment on his part. (GX 7 at 2; Tr. 211-12.) Applicant testified that he was removed because his project went over budget. He was replaced by another manager and assigned to manage another project. He was told by his supervisor that he should have been more aggressive in managing the budget. He admitted that he was unhappy about his removal for "the first week or two" (Tr. 212-13.) He denied that he received "counseling." He testified that he told his supervisor he was unhappy about his removal, his manager explained the reasons for his removal, and he realized that it was his manager's job to make the call. (Tr. 215-16.) He did not regard his removal as a demotion, and it did not affect his pay. (Tr. 289.) He does not believe it affected his professional standing, and he was not embarrassed by his removal. (Tr. 279-80.) His reassignment, counseling, and resentment were not alleged in the SOR.

In January 2009, Applicant used his employer's computer and email account to send an email to the White House, urging clemency for a former U.S. government employee who was convicted of spying for Israel and sentenced to life imprisonment. (GX 7 at 102.) Applicant testified he had no specific memory of the incident, but after seeing the investigative file he admitted sending the email. He believed that it was likely that an advocacy group sent an email to his work computer, asking him to sign and forward a prepared clemency request, and that he sent the email by "hitting a button." He admitted sending the email as humanitarian gesture, but he denied violating his company policy on personal use of company email. He believed that the convicted spy was guilty and deserving of severe punishment because he had betrayed his oath, but that the spy had been imprisoned for a long time and was in poor health. (GX 8 at 4; Tr. 197-99.) His employer's policy permits incidental personal use of unclassified company information technology (IT) assets as long as such use is on the employee's own time and does not interfere with the employee's job responsibilities. (GX 12.) Applicant testified that no one confronted him about the propriety of sending the email, and he did nothing to conceal it. (Tr. 203-04.)

In January 2010, Applicant was interviewed by agents of the AGA about the foreign contacts of his neighbor. The agents showed Applicant a photograph of a known Israeli intelligence officer with whom his neighbor had contacts. Applicant told the agents he did not recognize the person in the photograph or know his name. (GX 9 at 3.) Applicant told the agents that his neighbor had contacts with the wife of a U.S. employee who was convicted of spying for Israel.[1] (GX 9 at 3-4.)

Applicant was interviewed again by AGA agents on March 16, 2010. They questioned him about his brother's visit to the United States in October 2007, to surprise Applicant on his 60th birthday. (GX 8 at 1.) Applicant's neighbor also attended the birthday party and interacted with his brother. The AGA agents suspected that Applicant's brother had acted as a courier of equipment between his neighbor and the Israeli intelligence officer. Applicant told the AGA agents that he was unaware of any courier activity by his brother. However, Applicant told the AGA agents that both he and his brother frequently transported personal items to family or friends, because they were better quality or less expensive than Israeli equivalents. He recalled transporting a frying pan and clothing for his neighbor's daughter, a hard-wired telephone device for his son, and a tricycle for his grandson. (GX 7 at 5; GX 9 at 3.) He told the AGA agents that transporting items as a favor to a friend or casual acquaintance from the United States to Israel is common in the Jewish culture. (GX 8 at 2.)

The AGA agents also questioned Applicant about telephone records showing that the Israeli intelligence officer had called his cell phone on October 23, 2007, after his brother had returned to Israel. There is no evidence that the caller left a voicemail

[1] In light of the involvement of Applicant's neighbor with the wife of the convicted spy for Israel, it is likely that the neighbor was involved in sending the clemency request to Applicant's work email. It would not be unusual for friends and neighbors to share email addresses.

message. The AGA agents speculated that the purpose of the call could have been to notify Applicant that his brother had arrived safely in Israel.[2] (GX 7 at 4.) The telephone call was made from the same area code in the United States as Appellant's. There is no evidence that Applicant returned the call or had any contact with the intelligence officer. Applicant told the agents he had no recollection of the telephone call or any contact with a person identifying himself with the intelligence officer's name. (GX 8 at 3.)

At the hearing, Applicant testified that his son gave him his cell phone in 2004, when he returned to Israel to continue his Talmudic studies, and he continued to use the same cell phone number as his son's. He testified it was not unusual to receive cell phone calls from persons he did not know, and when it happened he simply hung up. (Tr. 240-43.) It is unclear whether the Israeli intelligence officer was trying to call Applicant or his son. His son had already returned to Israel to resume his Talmudic studies. The cell phone call from the Israeli intelligence officer is not alleged in the SOR.

On March 16, 2010, the AGA agents questioned Applicant about a "security incident" in June 2009, when one of his employer's security officials found him in a classified lab with the lights turned off. Applicant told the agents that he had no recollection of such an incident. He also told the agents that he has physical security responsibility for the lab in question, and he often shuts the door and turns out the lights as he exits. (GX 8 at 4.) There is no evidence that Applicant was questioned, counseled, or disciplined by his employer. Applicant denied the allegation regarding this incident in his answer to the SOR.

Applicant informed his facility security officer (FSO) that the AGA agents had questioned him about the June 2009 "security incident." (GX 3.) On March 25, 2010, almost a year after the incident and after Applicant told the FSO that the AGA agents were interested in the incident, the FSO filed an "Adverse Information/Suspicious Conduct Report" (GX 6), reciting the following:

> On June 9, 2009, a member of the IT security staff attempted to enter a closed area in order to audit a classified computer network. The staff member found the door to be open however no one had signed a logbook indicating their entry. Upon opening the door, all lights in the room were off and the lab was completely dark. The security employee turned to leave the lab when [Applicant], a program manager of [the defense contractor] appeared from the darkness to state that he was in the room. The security employee questioned his presence in the dark room and [Applicant] answered, "I forgot to turn on the lights." The security employee then asked why he had not signed to log book to indicate that he was in the

[2] The Israeli intelligence officer was the "handler" for a U.S. government employee (not the former government employee for whom Applicant signed the clemency petition) who pleaded guilty in 2009 to one count of conspiracy to act as an unregistered agent of Israel. (GX 7 at 3; Request to Take Administrative Notice, Enclosure V at 34 n. 116.)

room. [Applicant] did not answer the question but instead he went to the front of the door, signed the log book and left without further explanation.

During a personal subject interview (PSI) in October 2010, Applicant told the investigator that he frequently enters the classified lab as part of his managerial duties. To enter the lab, he swipes his access badge and then enters a numerical combination to unlock the door. He told the investigator that he is not required to sign a log because he is on the access list. (GX 4 at 4.) However, when he opens and closes a lab for which he is responsible at the beginning and end of a work day, he initials a log posted outside the lab. (Tr. 222.)

Applicant's former colleague, who was a program manager like Applicant, testified about the security procedures at their place of employment. He testified that if a lab custodian was the first person to open a secure lab, he would unlock a deadbolt by entering a numerical combination. Once inside the lab, the person would then punch in a code on a keypad inside the lab to turn off the alarm, which is activated by motion sensors, and sign a log sheet. To enter an unlocked lab, it was necessary to hold an access card up to a card reader and punch in a code. The doors to the labs are spring-loaded and automatically latch after a person enters. (Tr. 125-43.) Applicant's colleague testified that before the card readers and deadbolt combination locks were put in place, it was necessary to sign a log upon entering a classified lab. The current procedure does not require persons on the authorized access list to sign a log. Only persons not on the access list are required to sign a log. (Tr. 126-27.) No documentary evidence of the security procedures in place during June 2009 was submitted by either party at the hearing.

Applicant's former colleague testified that it would not be unusual for a person to re-enter a lab after turning out the lights to retrieve something. He testified that the labs are not completely dark, even with the lights turned off. (Tr. 127-28.)

Applicant's former colleague also testified that each lab custodian had a safe in the lab, with multiple authorized users. Each authorized user had a designated drawer inside the safe. He testified that it was not unusual for others to temporarily store classified documents in his safe rather than return them to the document library. Applicant's former colleague did not keep an inventory of the documents in his safe, although the document library kept records of the persons to whom classified documents had been given. (Tr. 145-46.)

Applicant submitted a table captioned "Approved Signature Authority for User Briefs." The table lists 15 programs conducted by his employer, and it reflects that Applicant is an approved signature authority for nine classified computer programs. (AX 7.) Applicant believed that the table was published for 2013 but he was not sure. (Tr. 276.) He testified that all the classified computers are located in labs, and that access to the computer network in a lab would include access to all the labs in which a specific computer program is located. (Tr. 189-93.)

After the June 2009 "security incident," a second security official went to the lab and found unclassified "hand sketches" or "doodles" pertaining to the project on which Applicant was working. The record does not indicate who made or possessed the "doodles." Applicant testified that they were not his and that he is not a doodler. (Tr. 220-21.) There was no evidence that any classified information was unprotected, removed, or otherwise compromised.

The same unidentified security official checked the company badge logs and concluded that Applicant's badge had been used to attempt access to areas to which Applicant does not have access. (GX 7 at 3.) The SOR does not allege when Applicant's attempts occurred. In his answer to the SOR and at the hearing, Applicant attempted to respond to the vague allegation. He denied intentionally trying to gain unauthorized access, but he admitted that there were times when he was unable to enter a lab with his security badge, either because the access rosters were not updated or because he could not remember which labs he was authorized to enter with his badge. He testified that he sometimes would be looking for another engineer in other labs, was not sure whether he was on the access roster for a particular lab, and would swipe his badge to determine if he had access. If he could not gain entry with his badge, he would knock on the door and inquire whether the person he was seeking was in the lab. If he was not on the access list, he would wait at the door while someone determined if the person he was seeking was in the lab.

The record does not reflect whether the unidentified security officer determined that Applicant attempted an unauthorized access based on computer records showing every use of his security badge or from the lack of Applicant's signature on the hand-written access logs in each lab. Applicant testified that he had never been told that he was suspected of attempting unauthorized access into a lab. (Tr. 195-97.)

At the hearing, Applicant testified that it would not be unusual for him to be in the lab with the lights dimmed. Some of the lights remain on even when the lights are "off." His usual practice is to turn the lights off, activate the alarm, and leave the lab. It also would not be unusual to walk back into the partially darkened lab to retrieve an item or make sure that documents were not unsecured. He also testified that persons listed on the access roster are not required to sign the log-in sheet. (Tr. 187-89.)

In July 2009, company security officials discovered that an internal security audit had been conducted in November 1983,[3] which found that Applicant had two documents in his safe that were not signed out to him. The auditors also found eight classified documents that did not have cover sheets protecting the classified information on the first pages. The report indicated that Applicant was given eight protective cover sheets for the uncovered documents. There is no evidence that any other action was taken by security officials. Neither side submitted any documentary evidence of the

[3] During November 1983, the Israeli intelligence who later called Applicant's cell phone in October 2007 was believed to be engaged in espionage at the location where Applicant worked.

employer's policies regarding signing for documents, storage of documents in a coworker's safe, or use of protective covers for documents locked in a safe inside a secured lab.

Applicant testified that he had no recollection of the security audit in November 1983, but he would not be surprised that it occurred. He testified that in November 1983 he was a department manager and had a safe in his office. When members of his staff worked beyond the closing time for the document library, he would permit them to store their classified materials overnight in his safe. [4] (Tr. 223-25.)

In August 2009, AGA investigators interviewed one of Applicant's former colleagues, who told them that Applicant often referred to himself as a "sabra" because of his place of birth. Applicant admitted using the term to describe himself. He explained that sabra is a desert cactus fruit, and persons born in Israel use it to describe themselves because the fruit is hard on the outside and soft on the inside. (GX 7 at 5; Tr. 230-33.)

Applicant's former colleague also told AGA investigators that Applicant commented at a social event, "We do this job for the money, not the patriotism." Applicant testified that he had no recollection of making the comment, and that he works for patriotism as well as the money. (GX 7 at 4; Tr. 237-38.)

Applicant's annual performance evaluations for 2009-2013 reflect that his performance was consistently rated as "achieved," meaning that he achieved all of his employer's performance objectives. (AX 1-5.) His ratings are the middle of five ratings, below "exceeded" and above two substandard ratings. (Tr. 292.) There are no negative comments in his performance evaluations regarding the conduct alleged in the SOR or his security awareness in general. In 2014, his team was nominated for a "Chairman's Award," because of its outstanding contributions to the company. (AX 6.)

A systems engineer, who has worked with Applicant from 1988 to 1999 and from 2003 until the present, submitted a statement describing Applicant as "an able professional and an excellent manager." He regards Applicant as "a very honest person, one to takes security seriously." (AX 13.)

[4] The SOR does not allege Applicant's social-religious contact with an Israeli officer in 1974 and his failure to report it, the presence in his safe of documents not signed out to him in November 1983, his failure to put protective cover sheets on classified documents in November 1983, or the telephone call from the Israeli intelligence officer in 2007. Conduct not alleged in the SOR may be considered to assess an applicant's credibility; to decide whether a particular adjudicative guideline is applicable; to evaluate evidence of extenuation, mitigation, or changed circumstances; to consider whether an applicant has demonstrated successful rehabilitation; or as part of a whole-person analysis. ISCR Case No. 03-20327 at 4 (App. Bd. Oct. 26, 2006). I have considered the conduct not alleged in the SOR for these limited purposes.

One of Applicant's colleagues, recently retired, has known him for about 40 years. He considered Applicant to be very diligent about protecting classified information.

Israel is a parliamentary democracy with a diversified, technologically advanced economy. Almost half of Israel's exports are high technology, including electronic and biomedical equipment. Israel is a close ally of the United States, and the United States is its largest trading partner.

Israel has been identified as a major practitioner of industrial espionage against U.S. companies. There have been instances of illegal export, or attempted illegal export, of U.S. restricted, dual-use technology to Israel. Israel has become a major global leader in arms exports, and the United States and Israel have periodically disagreed over Israeli sales of sensitive U.S. and Israeli technologies to third-party countries, including China.

The U.S. and Israel have close cultural, historic, and political ties. They participate in joint military planning and training, and have collaborated on military research and weapons development. Commitment to Israel's security has been a cornerstone of U.S. Middle East policy since Israel's creation in 1948.

Israel generally respects the rights of its citizens. When human-rights violations have occurred, they have involved Palestinian detainees or Arab-Israelis. Terrorist suicide bombings are a continuing threat in Israel, and U.S. citizens in Israel are advised to be cautious.

Israel considers U.S. citizens who also hold Israeli citizenship or have a claim to dual nationality to be Israeli citizens for immigration and other legal purposes. U.S. citizens visiting Israel have been subjected to prolonged questioning and thorough searches by Israeli authorities upon entry or departure.

Policies

"[N]o 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 applicants 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 AG. These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, an administrative judge applies these guidelines 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 and 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 that 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 made "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. Thus, a decision to deny a security clearance 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. 92-1106 at 3, 1993 WL 545051 at *3 (App. Bd. Oct. 7, 1993).

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 burden of proving a mitigating condition, and the burden of disproving it never shifts to the Government. *See* ISCR Case No. 02-31154 at 5 (App. Bd. Sep. 22, 2005).

An applicant "has the ultimate burden of demonstrating that it is clearly consistent with the national interest to grant or continue his security clearance." ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002). "[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

Guideline B, Foreign Influence

The SOR alleges that Applicant's son is a dual citizen of Israel and the United States (SOR ¶1.a). It also alleges that his brother and sister-in-law are dual citizens of the United States and Israel and reside in Israel (SOR ¶ 1.b), he has two nieces and

one nephew who are dual citizens of the United States and Israel and reside in Israel (SOR ¶ 1.c), and he has two nephews and one niece who are citizens and residents of Israel (SOR ¶ 1.d).

The security concern under this guideline is set out in AG ¶ 6 as follows:

> Foreign contacts and interests may be a security concern if the individual has divided loyalties or foreign financial interests, may be manipulated or induced to help a foreign person, group, organization, or government in a way that is not in U.S. interests, or is vulnerable to pressure or coercion by any foreign interest. 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.

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.

The totality of an applicant's family ties to a foreign country as well as each individual family tie must be considered. ISCR Case No. 01-22693 at 7 (App. Bd. Sep. 22, 2003). "[T]here is 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. 01-03120, 2002 DOHA LEXIS 94 at * 8 (App. Bd. Feb. 20, 2002); *see also* ISCR Case No. 09-06457 at 4 (App. Bd. May 16, 2011). There is a rebuttable presumption that contacts with an immediate family member in a foreign country are not casual. ISCR Case No. 00-0484 at 5 (App. Bd. Feb. 1, 2002).

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, "even friendly nations can have profound disagreements with the United States over matters they view as important to their vital interests or national security." ISCR Case No. 00-0317, 2002 DOHA LEXIS 83 at **15-16 (App. Bd. Mar. 29, 2002). Finally, we know friendly nations have engaged in espionage against the United States, especially in the economic, scientific, and technical fields. Nevertheless, 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).

The evidence establishes that Applicant's son is a citizen and resident of the United States and that he has never been a dual citizen of Israel and the United States. Thus, I conclude that Applicant has refuted the allegation in SOR ¶ 1.a.

Applicant admitted that his brother, sister-in-law, two nieces, and one nephew are dual U.S.-Israeli citizens. He also admitted that two nephews and one niece are citizens and residents of Israeli. The evidence submitted at the hearing indicates that his brother may have had contacts with an Israeli intelligence officer; and that one of his nieces was politically active in Israel, was employed by a high-ranking Israeli official, and continues to list the official as a reference on her professional resume. This evidence is sufficient to establish a heightened risk of foreign influence and a potential conflict of interest. Thus, I conclude that the following two disqualifying conditions under this guideline are established.

> AG ¶ 7(a): contact with a foreign family member, business or professional associate, friend, or other person who is a citizen of or resident in a foreign country if that contact creates a heightened risk of foreign exploitation, inducement, manipulation, pressure, or coercion; and
>
> AG ¶ 7(b): connections to a foreign person, group, government, or country that create a potential conflict of interest between the individual's obligation to protect sensitive information or technology and the individual's desire to help a foreign person, group, or country by providing that information.

Three mitigating conditions under this guideline are potentially relevant:

> AG ¶ 8(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;
>
> AG ¶ 8(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; and

AG ¶ 8(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.

AG ¶ 8(a) is not established. While Applicant and his brother have not been close for many years, they have a familial attachment, a sense of obligation to each other, and regular contact. Because of their relationship, regular contact, and Israel's record of industrial espionage, I cannot conclude that a potential conflict of interest is unlikely.

AG ¶ 8(b) is established. Applicant's sense of loyalty or obligation to his brother, his sister-in-law, his nieces, and his nephews is not "minimal," but it is outweighed by his deep and longstanding relationships and loyalties in the United States. He has lived in the United States since he was four years old. He has been a U.S. citizen for about 55 years. He has been a respected employee of a defense contractor for 42 years. His wife, son, daughter-in-law, and grandchildren are citizens and residents of the United States. He enjoys a reputation as an honest employee who is diligent about protecting classified information. He has not visited Israel since his son, daughter-in-law, and grandchildren returned to the United States in 2010. Applicant and his brother went their separate ways 30 years ago. While they share a sense of familial obligation, they have different loyalties and interests. I am satisfied that Applicant would resolve any conflict of interest in favor of the United States.

AG ¶ 8(c) is established for Applicant's sister-in-law, nieces, and nephews in Israel. However it is not established for his brother. Applicant has not overcome the presumption that communications with an immediate family member are not casual.

Guideline K, Handling Protected Information

The SOR alleges that, in June 2009, Applicant was found to have left the door of a secure lab open with the lights out, having failed to sign into the log book as required. (SOR ¶ 2.a). The amended SOR alleges that he used his security badge to attempt access to areas for which he did not have authorized access. (SOR ¶ 2.b). No dates are alleged in SOR ¶ 2.b.

AG ¶ 33 expresses the security concern pertaining to handling protected information: "Deliberate or negligent failure to comply with rules and regulations for protecting classified or other sensitive information raises doubt about an individual's trustworthiness, judgment, reliability, or willingness and ability to safeguard such information, and is a serious security concern."

Security violations are one of the strongest possible reasons for denying or revoking access to classified information, as they raise very serious questions about an applicant's suitability for access to classified information. Once it is established that an applicant has committed a security violation, he or she has a very heavy burden of demonstrating that he or she should be entrusted with classified information. Because security violations strike at the very heart of the industrial security program, an

administrative judge must give any claims of reform and rehabilitation strict scrutiny. *See* ISCR Case No. 03-26888 (App. Bd. Oct. 5, 2006).The frequency and duration of the security violations are aggravating factors. ISCR Case No. 97-0435 at 5 (App. Bd. July 14, 1998).

SOR ¶ 2.a alleges that Applicant left the door of a secured lab open. This allegation is contradicted by the evidence. While Applicant was in the lab, the deadbolt would have been unlocked, but the door would have automatically latched when it closed. There is no evidence that the door was propped open. The evidence also establishes that Applicant was not required to sign a log book except when he opened and closed the lab at the beginning and end of the work day. Applicant was the lab manager and authorized to be inside it. He would have been required to turn out the lights before activating the alarm, but even after the lights were "out" it was not completely dark. Applicant had no memory of the incident, but he and a former colleague described plausible reasons why he could have been in the dimly lighted lab, and both testified that they had remained in or returned to a darkened lab on several occasions. The fact that Applicant announced his presence to the security official, who had not noticed him, negates any suspicion that he was engaged in improper conduct. I conclude that SOR ¶ 2.a is not established.

SOR ¶ 2.b does not allege a date or a time period in which the conduct is alleged to have occurred. As such, it does not comply with the Directive ¶ E3.1.3, which requires that the SOR "shall be as detailed and comprehensive as the national security permits." Applicant's response to the allegation was hampered by the lack of specificity. However, he admitted that he sometimes would attempt to enter a lab by using his security badge if he was not sure whether he had access to the lab.

Two disqualifying conditions under this guideline are potentially applicable:

> AG ¶ 34(g): any failure to comply with rules for the protection of classified or other sensitive information; and
>
> AG ¶ 34(h): negligence or lax security habits that persist despite counseling by management.

Neither of these disqualifying guidelines is established. There is no evidence that "security violations" occurred in this case. The June 2009 incident was reported as a suspicious circumstance, not a violation, and Applicant gave a plausible and credible explanation, corroborated by the testimony of a former colleague, for his presence in the lab. He also gave a credible and plausible explanation for the documents in his safe that were not signed out to him. He gave a credible and plausible explanation for the possibility that he might have used his security badge to enter a lab where he did not have authorized access. The record contains no evidence of a requirement to attach protective covers to documents stored in a safe located in a controlled-access area. The record contains no evidence of a rule or policy prohibiting the holder of a security badge from using it to determine if he or she has been granted access to a secured area. No

violations of the applicable version DOD Manual 5220.22.-M, National Industrial Security Program Operating Manual (NISPOM) or any local regulation or policy were alleged or proven. There is no evidence that Applicant was counseled, admonished, or disciplined for his security habits. Applicant's failures to report a social-religious contact with an Israeli officer and failures to report personal foreign travel were not security violations, but rather violations of regulations intended to prevent security violations, and they are discussed below under Guideline E.

Guideline E, Personal Conduct

The SOR ¶ 3.a cross-alleges the conduct alleged in SOR ¶ 2.a under Guideline K. The amended SOR alleges that, in January 2009, Applicant violated company policy by using his company email account to contact the White House to seek clemency for a convicted spy (SOR ¶ 3.b). It also alleges that Applicant violated his company travel policy by failing to report his January 2009 travel to Israel (SOR ¶ 3.c). The concern under this guideline is set out in AG ¶ 15: "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 information. . . ."

The relevant disqualifying conditions are:

> AG ¶ 16(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 person may not properly safeguard protected information;
>
> AG ¶ 16(d): credible adverse information that is not explicitly covered under any other guideline and may not be sufficient by itself for an adverse determination, but which, when combined with all available information supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the person may not properly safeguard protected information. This includes but is not limited to consideration of . . . a pattern of dishonesty or rule violations; and
>
> AG ¶ 16(e): personal conduct, or concealment of information about one's conduct, that creates a vulnerability to exploitation, manipulation, or duress, such as . . . engaging in activities which, if known, may affect the person's personal, professional, or community standing.

SOR ¶ 3.a cross-alleged SOR ¶ 2.a. It is not established because no disqualifying conditions under Guideline K were established.

SOR ¶ 3.b is not established. The evidence establishes that Applicant joined in an email petition seeking clemency for a convicted spy. It also shows that his personal use of the email regarding a politically sensitive issue demonstrated bad judgment. However, it does not show that the company policy was violated.

SOR ¶ 3.c is not established. The evidence shows that a company policy requiring that personal foreign travel be reported was adopted during 2009, but it does not show that the policy was in effect in January 2009. The evidence is conflicting on whether Applicant reported his travel in 2010, but that failure to report was not alleged.[5]

I conclude that none of the allegations under Guideline E were proven by substantial evidence. Therefore, no disqualifying conditions under this guideline are raised.

Whole-Person Concept

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. In applying the whole-person concept, an 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. An administrative judge should consider the nine adjudicative process factors listed at AG ¶ 2(a):

> (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.

I have incorporated my comments under Guidelines B, K, and E in my whole-person analysis. Some of the factors in AG ¶ 2(a) were addressed under those guidelines, but some warrant additional comment.

[5] Even if Applicant failed to report his personal travel in January 2010, and if it had been alleged in the SOR, it would have been an isolated, minor infraction that happened more than four years ago, and it would be mitigated under AG ¶ 17(c) ("the offense is so minor, or so much time has passed, or the behavior is so infrequent . . . that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment.")

I have considered each of the incidents reflected in the record, whether or not alleged in the SOR. I have considered them individually and in totality, recognizing that apparently benign individual incidents can appear less benign when viewed as a series of unexplained coincidences.

Applicant was candid, sincere, and credible at the hearing. The record indicates that suspicions about Applicant's conduct arose from his neighbor's contacts with an Israeli intelligence officer, evidence that his brother may have been a courier between his neighbor and the Israeli intelligence officer, and the cell phone records reflecting that the Israeli intelligence officer called Applicant's cell phone. The AGA investigators interpreted Applicant's conduct and his prior history of work-related Israeli contacts through the prism of a counterintelligence investigation. Applicant's removal from a project manager position appeared to provide a motive for supporting Israeli intelligence operations. His ill-advised use of his company email to advocate clemency for a convicted spy was interpreted as sympathy for Israeli intelligence efforts. His comment about being motivated by money instead of patriotism was interpreted as a vulnerability. His reference to himself as a "sabra" could reflect a strong affinity for his birthplace. His presence in a darkened lab suggested an attempt to remove or copy documents.

The suspicious nature Applicant's conduct during the June 2009 "security incident" in the lab is rebutted by the FSO's report, reciting that Applicant announced his presence in the lab as the security agent began to leave the lab, unaware of Applicant's presence. If Applicant had been trying to remove or copy classified material, he would not have revealed his presence in the lab to a security agent who was unaware of his presence. Applicant's signing of the log sheet as he left the lab was consistent with his duty to secure the lab at the end of the work day.

The presence of classified documents in Applicant's safe that were signed out to others and his attempts to use his badge to enter labs where he was not on the access roster seemed suspicious because Applicant was suspected of having contact with a known Israeli agent, a premise not supported by the evidence. The suspicions based on Applicant's unreported trip to Israel in January 2009 are rebutted by the evidence that his travel to Israel was common knowledge among his coworkers and was solely for the purpose of being present at a religious event triggered by the birth of a grandson.

There is evidence that Applicant's neighbor and his brother may have had Israeli intelligence contacts. Their activities contributed to the "heightened risk" that Applicant might be faced with a conflict of interest. It is possible that the Israeli intelligence officer attempted to contact Applicant or his son. However, the record is devoid of evidence that any attempt to contact Applicant was successful. There is also no evidence that anyone attempted to contact Applicant after October 2007, and no evidence that he responded in any way to the October 2007 phone call. Without evidence supporting the premise that an Israeli intelligence officer successfully contacted Applicant, the various incidents alleged in the SOR and the incidents in GX 7 that were not alleged, considered individually as well as collectively, do not raise doubt about Applicant's trustworthiness and reliability,

After weighing the disqualifying and mitigating conditions under Guidelines B, K, and E, and evaluating all the evidence in the context of the whole person, I conclude Applicant has refuted the allegations in SOR ¶¶ 1.a, 2.a-2.b, and 3.a-3.c. He has mitigated the security concerns based on SOR ¶¶ 1.b-1.e. Accordingly, I conclude he has carried his burden of showing that it is clearly consistent with the national interest to continue his eligibility for access to classified information.

Formal Findings

I make the following formal findings on the allegations in the SOR:

Paragraph 1, Guideline B (Foreign Influence):	FOR APPLICANT
Subparagraphs 1.a-1.e:	For Applicant
Paragraph 2, Guideline K (Protected Information):	FOR APPLICANT
Subparagraphs 2.a-2.b:	For Applicant
Paragraph 3, Guideline E (Personal Conduct):	FOR APPLICANT
Subparagraphs 3.a-3.c:	For Applicant

Conclusion

I conclude that 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.

LeRoy F. Foreman
Administrative Judge