DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
[Redacted]	)	ISCR Case No. 11-15184
	)	
Applicant for Security Clearance	)	

Appearances

For Government: John Bayard Glendon, Esq., Department Counsel
For Applicant: Leslie McAdoo Gordon, Esq.

05/31/2013

Decision

FOREMAN, LeRoy F., Administrative Judge:

This case involves security concerns raised under Guidelines B (Foreign Influence) and E (Personal Conduct). Eligibility for access to classified information is denied.

Statement of the Case

Applicant submitted a security clearance application on August 18, 2011. On September 4, 2012, the Department of Defense (DOD) sent him a Statement of Reasons (SOR), alleging security concerns under Guidelines B and E. DOD acted under Executive Order 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; Department of Defense 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 September 7, 2012; answered it on September 27, 2012; and requested a hearing before an administrative judge. Department Counsel was ready to proceed on April 1, 2013, and the case was assigned to me on April 5,

2013. The Defense Office of Hearings and Appeals (DOHA) issued a notice of hearing on April 16, 2013, scheduling the hearing for May 2, 2013. I convened the hearing as scheduled. Government Exhibits (GX) 1 through 6 were admitted in evidence without objection. Applicant testified, presented the testimony of one witness, and submitted Applicant's Exhibits (AX) A through M, which were admitted without objection. DOHA received the transcript (Tr.) on May 10, 2013.

Administrative Notice

Department Counsel requested that I take administrative notice of relevant facts about Israel. The request is attached to the record as Hearing Exhibit (HX) I. I have taken administrative notice of the facts listed below.

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. The U.S. is Israel's 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.

Findings of Fact

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

Applicant is a 58-year-old senior principal network engineer for a defense contractor. He earned a bachelor's degree in computer science in 1983. He was employed by another defense contractor from May 1983 to July 2011. He has worked for his current employer since August 2011. (Tr. 35.) He has held a security clearance for about 25 years. (Tr. 7.)

Applicant married his current spouse in August 1986. They have two daughters, ages 24 and 25. Applicant and his spouse are native-born U.S. citizens. Applicant's parents and his spouse's parents are citizens and residents of the United States. Applicant and his spouse have no property or financial interests in Israel.

Before Applicant and his spouse married, his spouse's sister, a native-born U.S. citizen, became a citizen of Israel after marrying an Israeli. Her husband subsequently became a dual U.S.-Israeli citizen. His spouse's sister and her husband have three adult children: a daughter who is a dual U.S.-Israeli citizen and resides in Israel, and two sons, who are dual U.S.-Israeli citizens living and working in the United States. His spouse's sister and her husband visit family members in the United States two to four times a year. His spouse's sister and her husband are both employed by Israeli universities. She is a university librarian, and her husband is a university provost. Applicant and his spouse receive email from his spouse's sister about once a week. Applicant described his relationship with his wife's sister and her husband as "not a warm relationship," but civil. (Tr. 38-48; GX 3 at 5.)

In January 2005, Applicant violated a company security policy by failing to properly lock a secure area. The policy was to lock the door, hold a company badge to the badge reader next to the door, spin the door lock, and notify security by telephone to set the alarm. On one occasion, Applicant forgot to spin the lock, and a security guard noticed during the night that the lock had not been spun. No one had entered the area, and the alarm had not been triggered. Applicant was counseled and given remedial training. He did not remember whether he was verbally reprimanded. (GX 3 at 4.)

In February 2011, Applicant violated a company security policy regarding the changing of cryptographic keying material. He was required to change the encryption key every three months. The procedure requires that encryption keys be changed on both ends of the network. On February 1, 2011, Applicant changed the encryption key at his employer's end of the network and telephoned his counterpart at the other end of the network. His counterpart informed him that the key should not have been changed until March 1, 2011. Applicant contacted his communication security (COMSEC) custodian and reported that he had mistakenly installed the key a month early. The key is a paper tape stored in a canister. Once the tape is pulled out of the canister, it cannot be put back because of the design of the canister. (Tr. 66.) After consulting with the COMSEC custodian, he removed the new key, locked it in a safe, and reinstalled the old key in the encryptor. On March 1, 2011, the new key was reinstalled and the old key was destroyed. No data was transmitted improperly because Applicant's counterpart did not change the other key. (GX 3 at 3-4.)

Applicant's COMSEC manager had no recollection of the incident. When Applicant's current security investigation commenced, she contacted her superiors in the intelligence community and determined that the mistaken attempt to change the key a month early was not a reportable COMSEC incident. Consequently, no security investigation or disciplinary action was initiated. (GX 5.) Applicant disclosed the incident in his August 2011 security clearance application. He denied the allegation in SOR ¶ 2.b because it alleged that he actually used the new key before the prescribed date of use. The new key was prematurely loaded and then removed, but it was not used before its prescribed use date. (Tr. 70.)

Applicant began an outside business activity in the 1980s. It was a data back-up service for small businesses that he operated as a sole proprietorship. He worked in the evenings and notified his customers that he was not available during normal business hours. (Tr. 34.) He formally organized and incorporated his business on April 14, 2011. (AX B.)

Applicant acquired access to a proxy server in December 2010 or January 2011, to enable him to bypass his employer's restriction on access to web-based email and to have access to his personal email, using his company's unclassified computer. (GX 6 at 2; Tr. 49.) At that time, he was the lead member of the staff, responsible for understanding "the bigger picture of how things were configured and how things should work." He also was responsible for mentoring junior members of the team. (Tr. 85-86.) Initially, he used the proxy only for his personal email with family and friends, but then he started using it to communicate with clients of his data back-up service during normal business hours. He did not install or modify any programs or equipment on his company computer. (Tr. 56.)

Applicant knew that his use of a proxy server violated his employer's rules regarding use of a company computer. He knew that the purpose of preventing access to web-based email systems was to reduce the risk of introducing malware into the the company's information technology (IT) systems. However, because of his skill and experience, he was confident that he could recognize threats to the company's IT systems and that the risk of introducing malware was "extremely low." (Tr. 108-09.)

On April 21, 2011, a cyber-intelligence analyst conducting an investigation unrelated to Applicant discovered that several employees, including Applicant, were using proxy servers to circumvent the employer's filtering system and gain access to unauthorized Internet sites. (GX 6 at 14.) The computer incident response team monitored Applicant's computer for two weeks and identified 36 hours of suspected non-work activity on his computer. Applicant was interviewed on June 10, 2011, and he admitted using a proxy server to access his personal email accounts, running an outside business during the workday, and charging government contracts for time spent

on personal business.[1] Investigators determined that Applicant was multi-tasking during some of the 36 hours of suspected non-work activity. They concluded that, during the two-week period when Applicant's computer use was monitored, he billed 16.9 hours of personal use, worth about $1,076, to government contracts. (GX 6 at 5-6.)

On July 19, 2011, Applicant was given a termination notice for mischarging his time, misusing company computer assets, and violating his employer's security policies by using a proxy server to gain unfiltered access to the Internet from his company computer. (GX 6 at 53). He was given an opportunity to resign in lieu of termination, and on July 29, 2011, he resigned. (GX 6 at 4, 13.)

Applicant testified that resigning was a devastating experience. His father had worked for the same employer, his brother still works there, all his friends work there, and he had worked there for all of his adult life. He testified, "I think the hardest thing that I've ever had to do in my life is to go home without a job and explain what happened to my family." (Tr. 74.) When asked why he deliberately violated his employer's security rules, he said:

> I find it very difficult to understand how I could have rationalized doing what I was doing at that point. There is nothing that I can say that could possibly make that right. Looking back on it, I know that it was wrong for me to do that. I was in a position of responsibility. I had a top secret security clearance. I was in a position of trust. And to violate that and to do all of those things is not anything about who I was or who I continue to be. I cannot explain what was going through my head. I improperly rationalized in my head that what I was doing was not that bad. And I just fail to understand how I could have made the rationalization.

(Tr. 75-76.)

Applicant presented the testimony of a forensic examiner and consultant in computer investigations and data forensics. The witness testified that all of Applicant's activity involving use of a proxy server was processed on his own external server, and his employer's IT network merely provided the access port to the proxy service. The witness also testified that accessing personal email through a proxy server would not have altered, manipulated, or damaged the employer's network in any way. The witness opined that Applicant did not compromise or increase the vulnerability of his employer's IT system. (Tr. 117-24; AX A.)

Applicant testified that he uses his violation of his former employer's restrictions on Internet access as a "learning tool" in his new job, to make sure that those kinds of security violations do not happen. He has used his expertise to improve his new

[1] Portions of the report of investigation by Applicant's former employer reflect that his use of the proxy server was detected in April 2010, e.g., GX 6 at 14. However, the remainder of the report of investigation and Applicant's testimony at the hearing established that the events occurred in 2011.

employer's firewall and content filters to make sure that proxy servers cannot be used by company computers. He has also persuaded his new employer to install kiosk computers in the cafeteria to enable employees to access their web-based email accounts without compromising the company's IT systems. (Tr. 76-77.)

Applicant's duties at his new job are virtually the same as his previous job. His current employer is a subcontractor to his former employer, and he works closely with some of his former colleagues on defense contracts. (Tr. 78.)

Applicant testified that the reason for his job change is not generally known at his new place of employment. However, he has disclosed it to his human resources department, his manager, and his facility security officer (FSO). (Tr. 80.)

Applicant has continued to operate his personal business, but he testified that he is no longer looking for new business. He is still the sole member and sole employee of the company. (Tr. 112-13; AX B.)

The record does not reflect any actions by Applicant's former employer to revoke his clearance. The current review of Applicant's eligibility for a security clearance was triggered by his application to continue his clearance after being hired by his current employer. (Tr. 7.)

Applicant's current FSO has known him since August 2011 and has daily contact with him. The FSO has found Applicant to be extremely knowledgeable, trustworthy, loyal, and cognizant of the need to protect information. He believes that Applicant's prior conduct was a "one-time incident" and that Applicant has learned from that experience. The FSO recommends that Applicant be granted a security clearance. (AX C.)

An information system architect, who has known Applicant for 15 years as a supervisor, colleague, and friend, supports Applicant's application. He states that Applicant has demonstrated commitment to national security, commitment to information security, compliance with security policies and procedures, and trustworthiness and reliability as an employee, colleague, team leader, and in his personal relationships. He states that he is "at a loss to explain" Applicant's bypassing of corporate security controls because it is inconsistent with the "model of [Applicant's] behavior" that he has observed over the years. He regards the security violations in January 2005 and February 2011 as minor incidents, "within the normal range of incidents for people who have worked with classified networks for years." (AX D.)

Applicant's current supervisor, who has known him for more than 20 years, describes him as extremely dependable, reliable, security-conscious, hardworking, and efficient. He regards Applicant's circumvention of his company's Internet restrictions as a one-time incident, for which he is "incredibly remorseful." (AX F.)

A former colleague describes Applicant as very reliable, committed, and trustworthy. (AX G.) Applicant's family physician considers him to be kind, caring, and

thoughtful. (AX E.) His former COMSEC manager strongly supports his application for a clearance. (AX H.)

The president of the company by whom Applicant was formerly employed wrote a letter of recommendation for Applicant. He described Applicant as an "outstanding employee" who "made a lasting and positive impact upon the programs and customers he supported." (AX I.) At the hearing, Applicant testified that the president of the company wrote this letter after Applicant's father, who had been a senior executive of the company, asked him to write it. (Tr. 102-03.)

Throughout his career, Applicant has received numerous awards, commendations, and demonstrations of appreciation for his performance of duty. (AX J; AX M.) He was rated as a fully successful employee for two years between October 2007 and September 2009, and as an outstanding employee for the period from October 2002 to September 2003. His most recent performance appraisal from his current employer rated him as exceeding expectations, one level below the top rating of "exceptional" on a five-level scale. (AX K.)

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 brother-in-law, sister-in-law, and one niece are dual U.S.-Israeli citizens residing in Israel (SOR ¶¶ 1.a and 1.b), and his two nephews are dual U.S.-Israeli citizens residing in the United States (SOR ¶ 1.c). The security concern under this guideline is set out in AG ¶ 6:

> 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.

Three disqualifying conditions under this guideline are potentially relevant in this case:

> 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;
>
> 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; and
>
> AG ¶ 7(d): sharing 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.

AG ¶¶ 7(a) and (d) require 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.

When foreign family ties are involved, 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).

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).

Applicant's foreign family ties were created when his wife's sister, a native-born U.S. citizen, married an Israeli citizen, moved to Israel, and became a dual U.S.-Israeli citizen. Their three children are all dual U.S.-Israeli citizens, and the two boys have chosen to live and work in the United States. Although Applicant's ties to Israel are somewhat tenuous, the low threshold for "heightened risk" is met by the possibility that his wife's sister and her husband might seek to influence Applicant through his spouse. Thus, I conclude that there is sufficient evidence to raise AG ¶¶ 7(a) and (d) and create the potential conflict of interest in AG ¶ 7(b).

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.

Applicant has virtually no contact with his brother-in-law. His contacts with his sister-in-law are infrequent, but he has not rebutted the presumption that he has feelings of obligation to her. Applicant's sister-in-law could only exercise pressure or influence on him with the help of Applicant's wife, a circumstance that makes it unlikely that he would be confronted with a conflict of interest. Even assuming *arguendo* that a conflict of interest arose, I am satisfied that Applicant's deep and longstanding relationships and loyalties in the United States would cause him to resolve any conflict of interest in favor of the United States. I conclude that AG ¶¶ 8(a), (b), and (c) are established.

Guideline E, Personal Conduct

The SOR alleges that, in July 2011, Applicant resigned from his employment in lieu of termination for using a proxy server to improperly gain access to his personal email and for mischarging labor hours (SOR ¶ 2.a); that he violated a security procedure in February 2011 by prematurely using cryptographic keying material (SOR ¶ 2.b); and that he failed to properly secure a closed area in January 2005 (SOR ¶ 2.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."

Applicant's deliberate circumvention of his employer's rules restricting access to web-based email on company computers and his use of his employer's time and resources to operate a private business establish the following disqualifying conditions under this guideline:

> 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[2] 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 . . . (3) a pattern of dishonesty or rule violations; [and] (4) evidence of significant misuse of Government or other employer's time or resources; 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.

[2] Arguably, Applicant's conduct could have been alleged under Guideline K, ¶ 34(g) ("any failure to comply with rules for the protection of classified or other sensitive information") or under Guideline M, ¶ 40(e) ("unauthorized use of a government or other information technology system"). However, the Appeal Board has declined to apply the words, "not explicitly covered under any other guideline," as a limitation on the scope of Guideline E. ISCR Case No. 06-20964, 2008 WL 2002589 at *5 (App. Bd. Apr. 10, 2008).

The following mitigating conditions under this guideline are potentially relevant:

> AG ¶ 17(c): the offense is so minor, or so much time has passed, or the behavior is so infrequent, or it happened under such unique circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment;
>
> AG ¶ 17(d): the individual has acknowledged the behavior and obtained counseling to change the behavior or taken other positive steps to alleviate the stressors, circumstances, or factors that caused untrustworthy, unreliable, or other inappropriate behavior, and such behavior is unlikely to recur; and
>
> AG ¶ 17(e): the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress.

AG ¶ 17(c) is not established for the conduct alleged in SOR ¶ 2.a. Applicant's use of a proxy server to access his personal email account and his use of company time and resources to operate a private business were serious breaches of trust. He spent about 36 hours during a two-week period engaged fully or partially in personal business. He spent the equivalent of two full days, about 20% of his work time, operating his private business, and he billed that time to a government contract. He was in a leadership mission and entrusted with protecting the integrity of his employer's IT systems. When he discovered that content filtering system was vulnerable, he deliberately exploited it instead of fixing it. His conduct occurred frequently over a period of about four months, and it did not happen under unique circumstances making it unlikely to recur.

Applicant's use of the proxy server was recent. Although it ended about two years ago, it ended because he was caught in the act, not because he chose to stop. He has worked for his new employer for only about nine months, during which he has been under pressure to prove himself and keep his security clearance. Under the circumstances, I conclude that his misconduct has not been mitigated by the passage of time without recurrence. Thus, I conclude that AG ¶ 17(c) is not established for the conduct alleged in SOR ¶ 2.a.

On the other hand, the security violations in January 2005 and February 2011 were inadvertent, isolated violations. I conclude that AG ¶ 17(c) is established for the conduct alleged in SOR ¶ 2.b and 2.c.

AG ¶ 17(d) is not established for the conduct alleged in SOR ¶ 2.a. Applicant has acknowledged his behavior and he has ensured that his new employer's content filters will detect and block use of proxy servers. However, he continues to operate his private business, and the temptation and opportunity to use his employer's time and resources to run his private business still exists. While he is unlikely to resume use of a proxy server, I am not convinced that he is unlikely to use his employer's time and resources

for personal purposes in the future. On the other hand, the violations alleged in SOR ¶¶ 2.b and 2.c were inadvertent, isolated incidents, and they are unlikely to recur. Thus, I conclude that AG ¶ 17(d) is established for the conduct alleged in SOR ¶¶ 2.b and 2.c.

AG ¶ 17(e) is not established for the conduct alleged in SOR ¶ 2.a. Applicant has disclosed the reasons for leaving his previous employment to his human resources department, his manager, and his FSO, but he has not disclosed those reasons to his colleagues. On the other hand, the violations alleged in SOR ¶¶ 2.b and 2.c were inadvertent, isolated incidents of a nature described by one of Applicant's character witnesses as "within the normal range of incident for people who have worked with classified networks for years." As such, these two incidents do not make Applicant vulnerable to exploitation, manipulation, or duress. I conclude that AG ¶ 17(e) is established for the conduct alleged in SOR ¶¶ 2.b and 2.c.

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 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.

Applicant was a highly respected employee and held a security clearance for many years. He betrayed his employer's trust by exploiting the vulnerability of his employer's IT system for personal benefit. His misuse of his employer's time and resources continued until it was detected by cyber-intelligence analysts. He was embarrassed and remorseful at the hearing, but that embarrassment and remorse was attributable in part to the consequences of his conduct, not its inherent wrongfulness. While admitting that he breached his employer's trust, he attempted to downplay the potential harm to his employer's IT system. He believed that he could outwit anyone's effort to introduce malware into his company's IT system, but he was unable to outwit

his company's cyber-intelligence analysts, who uncovered his misconduct. He has not worked for his new employer long enough to demonstrate his current reliability, trustworthiness, and good judgment.

After weighing the disqualifying and mitigating conditions under Guidelines B and E, evaluating all the evidence in the context of the whole person, and mindful of my obligation to decide close cases in favor of national security, I conclude Applicant has mitigated the security concerns raised by his foreign family ties, but he has not mitigated the security concerns raised by his personal conduct. Accordingly, I conclude he has not 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.c:	For Applicant
Paragraph 2, Guideline E (Personal Conduct):	AGAINST APPLICANT
Subparagraph 2.a:	Against Applicant
Subparagraphs 2.b-2.c:	For Applicant

Conclusion

I conclude that it is not clearly consistent with the national interest to continue Applicant's eligibility for a security clearance. Eligibility for access to classified information is denied.

LeRoy F. Foreman
Administrative Judge