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.

08/15/2013

_____

Decision on Remand

_____

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.

On May 31, 2013, I denied Applicant's application to continue his security clearance. I concluded that the security concerns based on foreign influence and two instances of personal conduct alleged in SOR ¶¶ 2.b and 2.c were mitigated, but that the personal conduct alleged in SOR ¶ 2.a was not mitigated. SOR ¶ 2.a alleges that Applicant resigned from his employment in lieu of termination following his improper use of the Internet to access personal web email by use of a proxy and mischarging the hours of labor billed to a client of his employer.

Applicant timely appealed my adverse decision, and on July 25, 2013, the Appeal Board remanded the case for a new decision. The basis for the remand was the following language in my analysis of the applicability of the mitigating condition in AG ¶ 17(c)[1] to Applicant's conduct:

> 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.

Applicant challenged my comment that he had worked for his new employer "for only about nine months," and he cited the record evidence that he had worked for his new employer since August 2011. The Appeal Board found his challenge persuasive and also noted my finding of fact that Applicant had worked for his current employer since August 2011, a period of about 21 months. The Appeal Board concluded that my analysis of AG ¶ 17(e) was erroneous, and it was unable to conclude that the error was harmless. Accordingly, the Appeal Board remanded the case to me for a new decision.

Findings of Fact

I adhere to the findings of fact in my initial decision. The following findings of fact from my initial decision in this case are relevant to the issue on remand.

[1] "[T]he 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."

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. He has held a security clearance for about 25 years. (Decision at 3.)

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. He formally organized and incorporated his business on April 14, 2011. (Decision at 4.)

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. 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. 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. (Decision at 4.)

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 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." (Decision at 4.)

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. 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. 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. (Decision at 4-5.)

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. He was given an opportunity to resign in lieu of termination, and on July 29, 2011, he resigned. (Decision at 5.)

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." 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.

(Decision at 5.)

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.[2] (Decision at 5.)

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 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. (Decision at 5-6.)

[2] The expert testimony was presented to corroborate Applicant's testimony that he did not install or modify anything on his employer's computer, that he did not compromise the classified IT system, and that he was confident that his technical skills enabled him to prevent any malware from entering his employer's IT system. (Tr. 56-57, 59, 107-08.) It also provided the basis for his counsel's closing argument that his violations were "very technical" and did not violate the integrity of his employer's IT system. (Tr. 138-39.)

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. (Decision at 6.)

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). (Decision at 6.)

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. (Decision at 6.)

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. (Decision at 6.)

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. (Decision at 6.)

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. (Decision at 6.)

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." (Decision at 6.)

A former colleague describes Applicant as very reliable, committed, and trustworthy. Applicant's family physician considers him to be kind, caring, and thoughtful. His former COMSEC manager strongly supports his application for a clearance. (Decision at 6-7.)

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." 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. (Decision at 7.)

Throughout his career, Applicant has received numerous awards, commendations, and demonstrations of appreciation for his performance of duty. 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. (Decision at 7.)

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

I adhere to my favorable resolution of the Guideline B allegations in SOR ¶¶ 1.a through 1.c and the Guideline E allegations in SOR ¶¶ 2.b and 2.c, for the reasons set out in my initial decision. The scope of this decision on remand is limited to my adverse decision on SOR ¶ 2.a, which alleged 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.

I adhere to the determination in my initial decision that 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 established 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 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.

I also adhere to the determination in my initial determination that the following mitigating conditions 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.

The narrow issue in this remand is the impact of my reference to a period of "about nine months" in my analysis of the applicability of AG ¶ 17(c). The reference to "about nine months" was an inadvertent misstatement that was not consistent with my findings of fact. However, it did not affect my determination that Applicant's conduct was not mitigated by the passage of time without recurrence.

As noted by the Appeal Board, there are no "bright line" rules for determining when conduct is "recent." The determination must be based on a careful evaluation of the totality of the evidence. *See* ISCR Case No. 02-24452 at 6 (App. Bd. Aug. 4, 2004). If the evidence shows "a significant period of time has passed without any evidence of misconduct," then an administrative judge must determine whether that period of time demonstrates "changed circumstances or conduct sufficient to warrant a finding of reform or rehabilitation." *Id*.

The Appeal Board noted that I found in my original decision that Applicant had worked for his current employer since August 2011. In my analysis, I relied on this finding of fact, and I concluded that the passage of time since his misconduct not sufficient to mitigate his conduct, because during the period from August 2011 until the

record closed he was "under pressure to prove himself and keep his security clearance." My analysis of AG ¶ 17(c) also included the following comments:

> 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 [position] and entrusted with protecting the integrity of his employer's IT systems. When he discovered that [the] 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.

(Decision at 12.)

Furthermore, my adverse decision was not based solely on the analysis of AG ¶ 17(c). In my analysis of AG ¶ 17(d), I concluded that Applicant is unlikely to resume use of a proxy server to bypass his employer's content filters, but I was not convinced that he is unlikely to use his employer's time and resources for personal purposes. (Decision at 12-13.) In my analysis of AG ¶ 17(e), I noted that Applicant had disclosed the reasons for leaving his previous employment to his human resources department, his manager, and his facility security officer, but he had not disclosed them to his colleagues. (Decision at 13.) In my whole-person analysis, I noted the following:

> 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.

(Decision at 13-14.)

In accordance with the terms of the remand, I have reconsidered my decision in light of the inadvertent misstatement in my analysis of AG ¶ 17(c). Based on all the evidence, I am not satisfied that concerns about his current reliability, trustworthiness, and good judgment have been mitigated by the passage of time. I am not convinced that his circumvention of his employer's rules and misuse of his employer's time and

resources for personal purposes will not recur once the pressure of protecting his security clearance is removed. Accordingly, I conclude that Applicant has not mitigated the security concerns raised by the conduct alleged in SOR ¶ 2.a.

Formal Findings

I adhere to my findings in the original decision, which were as follows:

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