DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
XXXXX, Xxxxxx Xxxx	)	ISCR Case No. 12-00738
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Daniel F. Crowley, Esquire, Department Counsel
For Applicant: Leslie McAdoo Gordon, Esquire

08/30/2013

Decision

METZ, John Grattan, Jr., Administrative Judge:

Based on the record in this case,[1] Applicant's clearance is granted.

On 5 June 2013, the Department of Defense (DoD) issued a Statement of Reasons (SOR) to Applicant listing security concerns under Guideline E, Personal Conduct.[2] Applicant timely answered the SOR, requesting a hearing before the Defense Office of Hearings and Appeals (DOHA). DOHA assigned the case to me 25 July 2013, and I convened a hearing 22 August 2013. DOHA received the transcript (Tr.) 30 August 2013.

[1]Consisting of the transcript (Tr.), Government exhibits (GE) 1-4, and Applicant exhibits (AE) A-M.

[2]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) effective within the DoD on 1 September 2006.

Findings of Fact

Applicant admitted being reprimanded by his company in May 2008 for failing to secure a closed area on several occasions (SOR 1.a). He denied failing to turn off his cell phone in a closed area (SOR 1.b) and failing to timely report counseling he received in May 2010 (SOR 1.c). He is a 38-year-old senior software engineer employed by a Government contractor since February 2003. He has never married. He seeks reinstatement of the security clearance he has held largely without incident since 1998.

Applicant has been the subject of favorable background investigations in August 1998, May 2003, January 2008, and March 2012. Consequently, he has had both clearance and access as necessary.

In May 2008, Applicant was reprimanded by his employer for failing to strictly follow company security protocols in securing a closed area on several occasions. Applicant reported these failures to his employer at the time of his periodic reinvestigation in early 2008. Applicant's company took no other disciplinary action against him, and his clearance was renewed by the Government after completing the background investigation.

Company security protocols for the space Applicant worked in required the last person in the space to completely secure the space when leaving, regardless of the length of time someone left the space. That required every classified computer in the space to be logged off, screen locked, or in password-protected mode. Classified printers had to be powered off, drawers pulled out, and checked to ensure that no classified documents were on them. All safes had to be checked to ensure they were locked. The motion-detector alarm had to be armed. The security protocols further required the last person leaving the space to engage the combination lock by spinning the dial upon exiting. The space was also secured at all times by a badge and PIN lock.

The software division Applicant worked in had responsibilities in time zones that worked hours past the normal closing time in Applicant's location. Because Applicant was the only unmarried employee in that division, he frequently stayed late to handle issues from offices that were still open, allowing his married colleagues to go home at the normal closing time. For several years before the 2008 periodic reinvestigation, Applicant failed to complete the last step in the security protocols (spinning the dial on the combination lock) when he left the space for short periods of time to go to the restroom or buy something from the vending machine. He was typically absent for about five minutes on these occasions.

Applicant failed to spin the dial on the combination lock for two reasons. First, he considered the requirement unnecessary for short periods given that access to the space was restricted to employees who had a coded security badge that would open the electronic lock when the employee swiped the access card and entered a user-specific PIN. Second, he frequently encountered trouble getting the combination lock to

open, causing him to be away from his work space for significantly longer than he expected. Applicant always engaged the combination lock when he left work for the day.

When Applicant began his periodic reinvestigation in 2008, he disclosed his security failures to his employer. He was reprimanded by his employer in May 2008, and he has not repeated this conduct since. Applicant reported this conduct on both his August 2011 (GE 1) and February 2013 (GE 2) clearance applications.

The security protocols for Applicant's work space also required employees to leave their cell phones outside the space, in cubbyholes provided by the employer for that purpose. Applicant habitually turned off his cell phone as soon as he parked at work in the morning, but on about six occasions between August 2009 and March 2013, he brought his cell phone into his work space. He usually discovered that he had done so within a matter of minutes. On each occasion he immediately put his cell phone out of the work space as required and notified his facility security officer (FSO) either by email or in person (AE A). Applicant was apparently not the only employee in the division to have this issue on occasion, as the FSO noted her own shortcoming in not posting a reminder warning outside the space. Applicant's employer took no disciplinary action against him for any of these infractions.

In early 2010, Applicant's division was short staffed, and he was feeling some anxiety about the work requirements he was subject to. He spoke to his supervisor, who referred him to the company employee assistance service (EAS), which in turn referred him to a counselor out in the community. Applicant saw a psychologist once in May 2010. The psychologist found no reason for Applicant to be concerned and did not recommend any further treatment. Applicant wondered whether he was required to report this counseling to anybody at work, but was unable to find any definitive answer about reporting this counseling session to his employer or the Government. He also thought the session might not be reportable since no ongoing treatment occurred. Consequently, he did not report this counseling session outside his supervisor or EAS.

In early 2011, Applicant received his annual company security briefing, during the course of which he realized that he should have reported the counseling session to his FSO. He did so immediately, triggering the February 2011 incident report (GE 3) that ultimately lead to the current adjudication. Applicant reported this counseling session on both clearance applications contained in the record.

Applicant has an excellent employment record (AE I-J). He has received many awards, certificates, and regular security briefings (AE L-M). His many work and character references consider him honest and trustworthy, and note that he is one of the most security conscious employees at the company (AE B-H).

Policies

The adjudicative guidelines (AG) list factors for evaluating a person's suitability for access to classified information. Administrative judges must assess disqualifying and

mitigating conditions under each issue fairly raised by the facts and situation presented. Each decision must also reflect a fair, impartial, and commonsense consideration of the factors listed in AG ¶ 2(a). Any one disqualifying or mitigating condition is not, by itself, conclusive. However, specific adjudicative guidelines should be followed where a case can be measured against them, as they represent policy guidance governing access to classified information. Considering the SOR allegations and the evidence as a whole, the relevant adjudicative guideline is Guideline E (Personal Conduct).

Security clearance decisions resolve whether it is clearly consistent with the national interest to grant or continue an applicant's security clearance. The Government must prove, by substantial evidence, controverted facts alleged in the SOR. If it does, the burden shifts to applicant to refute, extenuate, or mitigate the Government's case. Because no one has a right to a security clearance, the applicant bears a heavy burden of persuasion.

Persons with access to classified information enter into a fiduciary relationship with the Government based on trust and confidence. Therefore, the Government has a compelling interest in ensuring each applicant possesses the requisite judgement, reliability, and trustworthiness of those who must protect national interests as their own. The "clearly consistent with the national interest" standard compels resolution of any reasonable doubt about an applicant's suitability for access in favor of the government.[3]

Analysis

The Government failed to establish a case for disqualification under Guideline E. The facts alleged in the SOR most arguably constitute security violations, yet this case was not alleged as a security violation case under Guideline K, properly so in my view. What remains are three allegations that do not support a case for disqualification under Guideline E. The facts alleged in the SOR do not constitute evidence of falsification cognizable under ¶¶16.(a) or 16.(b). Department Counsel acknowledged that ¶¶16.(e), 16.(f), and 16.(g) did not apply. ¶16.(c) fails as a grounds for disqualification because what adverse information there is does not fall into several adjudicative issue areas.[4] ¶16.(d) fails as a grounds for disqualification because the conduct alleged explicitly falls under Guideline K, Handling Protected Information. Both ¶¶16.(c) and 16.(d) fail as grounds for disqualification because they do not support 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.

[3] *See*, *Department of the Navy v. Egan*, 484 U.S. 518 (1988).

[4] ¶ 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;

A reasonable reading of the facts surrounding these allegations confirms the conclusions of the whole-person evidence in this case: that Applicant is extremely security conscious in his job. Without condoning his failure to complete the last step in the security protocols for securing his workspace before May 2008, it is difficult to argue that his actions lacked common sense. Something which is often more important than strictly following regulations. Moreover, Applicant reported this misconduct rather than conceal it, was reprimanded for it by his employer, and he never repeated the conduct again. Similarly, we know of Applicant's occasional failure to leave his cell phone outside his work space because he reported each instance to his FSO, who took no action against Applicant except to note the infraction. Finally, we know of Applicant's single counseling session because he reported it to his employer as a result of his annual security briefing. Here again, Applicant's employer took no disciplinary action against Applicant for not reporting this counseling session. Applicant's actions are the actions of an employee who takes his security responsibilities seriously.

Finally, the most serious of Applicant's conduct occurred over five years ago, and has not been repeated. Applicant's cell phone issues amount to administrative infractions that Applicant has addressed by leaving his cell phone in his car when he gets to work. Further, although Applicant concluded that he should have reported his single counseling session when taking his annual security briefing, I do not think he was necessarily incorrect by not reporting it, for the reasons he cited. I note that neither Applicant's supervisor (who referred him to the EAS), or the EAS contact (who referred him to the counseling center), considered those referrals reportable to the FSO as part of their own security obligations. The Government's evidence does not demonstrate that Applicant was required to report this counseling to anyone in the company beyond his supervisor or the EAS contact, both of whom were presumably aware of the session. The fact that the clearance application contains a section where Applicant could, and did, report this single counseling session does not establish that he was required to do so. Put another way, under the circumstances of Applicant's counseling session (with no follow-up counseling), his reporting the session, while prudent, does not appear to have necessarily been required. I resolve Guideline E for Applicant.

Formal Findings

Paragraph 1. Guideline E:	FOR APPLICANT
Subparagraphs a-c:	For Applicant

Conclusion

Under the circumstances presented by the record in this case, it is clearly consistent with the national interest to grant or continue a security clearance for Applicant. Clearance granted.

JOHN GRATTAN METZ, JR
Administrative Judge