DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 14-02373
	)	
	)	
Applicant for Security Clearance	)	

For Government: Caroline Heintzelman, Esquire, Department Counsel
For Applicant: *Pro Se*

10/07/2015

_____

Decision

_____

DAM, Shari, Administrative Judge:

Between November 2009 and February 2013, Applicant committed nine security infractions, all of which he self-reported to his employer. Since taking corrective steps, he has not had another incident. Although he failed to disclose all of the infractions on his most recent security clearance application, his innocent explanation for the non-disclosure was credible. Resulting security concerns are mitigated. Eligibility for access to classified information is granted.

Statement of the Case

In April 2013 Applicant submitted a security clearance application (SCA) for re-investigation. On January 8, 2015, the Department of Defense Consolidated Adjudications Facility (DoD CAF) issued Applicant a Statement of Reasons (SOR) detailing security concerns under Guideline K (Handling Protected Information) and Guideline E (Personal Conduct). The action was taken 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 the came into effect in the Department of Defense on September 1, 2006.

On February 24, 2015, Applicant answered the SOR in writing and requested a hearing before an administrative judge (Answer). On April 27, 2015, the Defense Office of Hearings and Appeals (DOHA) assigned the case to me. On June 5, 2015, DOHA issued a Notice of Hearing. The case was heard on June 30, 2015, as scheduled. Department Counsel offered Government Exhibits (GE) 1 through 4 into evidence without objection. Applicant testified and offered Applicant Exhibits (AE) A through C into evidence without objection. The record remained open until July 20, 2015. Applicant subsequently requested an extension of said date, and it was extended to July 24, 2015, without objection from Department Counsel. Applicant timely submitted a memorandum with seven attachments, which I marked as AE D and admitted into evidence without objection from Department Counsel. DOHA received the hearing transcript on July 9, 2015.

Findings of Fact

In his Answer, Applicant admitted all allegations contained in SOR ¶ 1 and denied the allegations contained in SOR ¶ 2. His admissions are included in the findings of fact.

Applicant is 58 years old and married for 32 years. They have two adult children. He has a bachelor's and master's degree in engineering. He began working for his current employer, a defense contractor, in 1980. He has held a security clearance continuously since then. He is a manager and supervisor for 14 employees. (Tr. 23-27, 31.) He currently holds a Top Secret clearance and has access to the special access program (SAP), and the sensitive compartmented information (SCI) channel. (Tr. 9, 86.)

Applicant works in secured areas of his employer's office. According to security regulations, he is prohibited from bringing a cell phone or an unclassified work computer into the secured areas. (Tr. 32-34.)

Between November 2009 and early February 2013, Applicant failed to comply with security regulations pertaining to introducing prohibited items in a secured area eight times. In December 2009, October 2010, May 2012, August 2012, and February 2013, he forgot to take his cell phone out of his jacket before entering the secured space. In November 2009, November 2011, and December 2012, he forgot to take an unclassified laptop out of his backpack before entering the secured space. He promptly reported every incident, except the December 2012 incident, to the company's security officials as required by its policies and procedures. The December 2012 incident occurred during a Christmas luncheon on December 14, 2012, and he reported it on January 3, 2013. After ruminating in the two interim weeks about having committed a potential security infraction, he recalled that he must have left his laptop in his backpack

on that day when he walked into the secured area. (Tr. 51-53.) He said no one would have known of any of the infractions, if he had not self-reported.[1] (Answer.)

In mid-February 2013 Applicant used a piece of paper from an unclassified stack of paper located in the secured area to write some unclassified notes. He subsequently put the paper in his pocket and took it home. When he looked at it while home, he turned the paper over and discovered that it had "programmatic security markings associated with our proprietary program printed top and bottom of the unused side." (Answer.) He immediately telephoned the security official and reported the incident. He then secured it, and drove back to his office where he placed the paper in a secure safe. A subsequent investigation determined that the information on the paper was unclassified. (AD D: Enc. 4.) This was the ninth and last security infraction. (Tr. 60-63.)

Applicant received a verbal warning after the November 2009 incident. (Tr. 41.) After the December 2009, February 2010, and October 2010 incidents, he received written warnings. (Tr. 43-45.) He received verbal warnings after the November 2011 and May 2012 incidents. (Tr. 46.) He received a written warning after the August 2012 incident. (Tr. 48.) He received a verbal warning after the December 2012 incident. He received a written reprimand after the mid-February 2013 incident involving the removal of a piece of paper. (Tr. 61.) In April 2013 he received a corrective action memorandum and lost a day's pay as a result of the two February 2013 security incidents. (Tr. 57, 63; GE 4.)

Applicant explained that the incidents occurred because he was normally in a hurry in the morning when he arrived at work and did not remove his coat (containing his cell phone) or backpack (containing an unclassified laptop) before entering the secured area, which was about 10 feet from the building entrance door. In addition to rushing into work, he was not sleeping well because of painful wrist problem. He believed these factors and other stress contributed to the incidents. (Tr. 67-71.)

Applicant said that he was not required to take additional training in security procedures after the incidents, but he did meet with the security and program managers, who told him to figure out a way to change his morning behavior in order to stop the security incidents. (Tr. 64.) He subsequently established a strict behavioral pattern to avoid similar mistakes. He no longer puts the laptop in his backpack and he leaves his cellphone in his car and not in his coat. (Tr. 36-37.)

When Applicant completed a security clearance application (SCA) in April 2013, he disclosed two of the nine work-related security infractions, which resulted in discipline or a warning: the one occurring in December 2012, and the one occurring in

[1] Applicant noted that his mistakes are considered security infractions and not security violations. A security violation involves the loss or potential compromise of classified information. A security infraction is any incident that is "not in the best interest of security that does not involve the loss, compromise, or suspected compromise of classified information." (AE D at 2.)

early February 2013.[2] Applicant explained that he assumed that his employer had reported the infractions to the Government or Office of Personnel Management (OPM) after he reported them to his employer. He thought that his employer's security database was interconnected with the Government's security database. However, when he completed the SCA in April 2013, he was not certain that the Government had received information about the December 2012 or February 2013 infractions, so he disclosed them. (Tr. 74-76, 83-84; Answer.) He acknowledged that he mistakenly did not disclose the February 2013 piece of paper incident in the SCA. (Tr. 76.)

During an investigative interview, Applicant assumed that the investigator had all of the information from his employer's database and the disclosures in his April 2013 SCA. When the investigator asked, toward the end of the interview, if Applicant had any other infraction to report, Applicant said "nothing beyond the paper." The investigator appeared surprised by his answer and Applicant then showed the investigator the corrective action memo he had received in April 2013. (Tr. 77.) Applicant said that in response to the investigator's surprise he should have asked the investigator what information he had in his file pertinent to the security infractions. "But in that case, I made the assumption it was merely a timing issue relative to when the investigator asked for and received information" from his employer's database. (Tr. 80-82; AE D.)

Applicant denied that he intentionally attempted to deceive the Government. (Tr. 85.) He clearly understood the potential consequences for committing security infractions when he reported them, including the possibility that he could be terminated. He knew that it was his responsibility to report the incidents regardless of the outcome. (Tr. 86; AE D.) He stated that "there was never a data spill or compromise for our national security . . . The Government customer in this case is aware of all of the infractions and has accepted the risk for all of these occurrences." (AE D.) He wrote:

> At no time did I attempt to deceive, mislead or preclude from being forthright when questioned by any investigator in regard to any security incidents. I made a human error in regard to failing to report security incidents in my [SCA] that I previously thought had been reported through program channels to the U.S. Government. (AE D.)

Applicant submitted four letters of recommendation. The Director of Proprietary Programs, who has known Applicant for 24 years, wrote that he strongly supports Applicant. He said that Applicant has always taken security issues seriously. Applicant's security professional, who has known Applicant for over 30 years, stated that Applicant is ethical, forthcoming, and a technical leader in the company. He noted that Applicant's self-reporting of the incidents attests to Applicant's character and commitment to security. He stated that Applicant demonstrated for the past two years that the corrective steps he instituted have worked, and that there have not been any additional

[2] In his SCA, Applicant wrongly listed a February 2013 infraction as having occurred in March 2013. (Tr. 74.)

incidents since February 2013. He also stated that he never considered Applicant a security risk, irrespective of the security infractions. (AE D.)

An associate, who has known Applicant for 12 years, strongly recommends that Applicant maintain his security clearance. He said that Applicant takes security responsibilities seriously, as indicated by his self-reporting and exhibited by the corrective actions he has taken over the past couple years. A human resources employee, who has served as Applicant's resource person from 2004 to 2014, noted that Applicant demonstrated integrity by immediately coming forth with his infractions. He said that Applicant is careful to check that he does not take prohibited items into the secured area after arriving at work. (AE D.)

Applicant testified candidly and credibly. He takes full responsibility for failing to comply with security procedures. Since the last incident in February 2013, he has tried to "slow down." (Tr. 47.) He emphasized that he did not attempt to hide the infractions from the Government. (Tr. 86.)

Policies

When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the adjudicative guidelines (AG). In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially disqualifying conditions and mitigating conditions, which are useful in evaluating an applicant's eligibility for access to classified information.

These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, these guidelines are applied in conjunction with the factors listed in AG ¶ 2 describing the adjudicative process. The administrative judge's overarching adjudicative goal is a fair, impartial, and commonsense decision. According to AG ¶ 2(c), the entire process is a conscientious scrutiny of a number of variables known as the whole-person concept. The administrative judge must consider all available, reliable information about the person, past and present, favorable and unfavorable, in making a decision.

The protection of the national security is the paramount consideration. AG ¶ 2(b) requires that "[a]ny doubt concerning personnel being considered for access to classified information will be resolved in favor of national security." In reaching this decision, I have drawn only those conclusions that are reasonable, logical, and based on the evidence contained in the record. Likewise, I have avoided drawing inferences grounded on mere speculation or conjecture.

According to Directive ¶ E3.1.14, the Government must present evidence to establish controverted facts alleged in the SOR. Under Directive ¶ E3.1.15, an "applicant is responsible for presenting witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by the applicant or proven by Department Counsel, and has the ultimate burden of persuasion as to obtaining a favorable clearance

decision." Section 7 of Executive Order 10865 provides that adverse decisions shall be "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned."

A person applying for access to classified information seeks to enter into a fiduciary relationship with the Government predicated upon trust and confidence. This relationship transcends normal duty hours and endures throughout off-duty hours. The Government reposes a high degree of trust and confidence in individuals to whom it grants access to classified information. Decisions include, by necessity, consideration of the possible risk the Applicant may deliberately or inadvertently fail to protect or safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation as to potential, rather than actual, risk of compromise of classified information.

Analysis

Guideline K, Handling Protected Information

The security concern relating to the guideline for handling protected information is set out in AG ¶ 33:

> 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.

AG ¶ 34 describes two conditions that could raise a security concern and may be disqualifying based on the facts of this case:

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

Applicant admitted that on nine occasions he failed to comply with security procedures, eight of which occurred after he had received either a verbal or written warning for the earlier infractions. Those nine instances indicated lax security habits. The foregoing disqualifications have been raised.

After the Government produced substantial evidence of those disqualifying conditions, the burden shifted to Applicant to produce evidence and prove mitigation. AG ¶ 35 provides two conditions that could mitigate security concerns in this case:

(a) so much time has elapsed since the behavior, or it has happened so infrequently or under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or good judgment; and

(b) the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities.

Applicant's last security infraction occurred in February 2013, about two and a half years ago. Given the steps he has taken to prevent similar incidents and evidence that his newly established steps are effective, it is unlikely that similar behavior will recur, such that his prior behaviors do not cast doubt on his current reliability or trustworthiness. According to Applicant's security manager, Applicant has responded favorably to the corrective steps he implemented to guard against bringing his cell phone or laptop into secured areas. These facts coupled with Applicant's committed attitude in executing his security responsibilities establish mitigation under AG ¶ 35(a) and AG ¶ 35(b).

Guideline E, Personal Conduct

AG ¶ 15 expresses the security concern pertaining to personal conduct:

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. Of special interest is any failure to provide truthful and candid answers during the security clearance process or any other failure to cooperate with the security clearance process.

The Government alleged in SOR ¶¶ 2(a) and 2 (b) that Applicant deliberately falsified answers to questions on his April 2013 SCA, by failing to disclose information regarding past security infractions, and during a May 2013 investigative interview. The Government contended that those falsifications constituted potential disqualifying conditions under AG ¶ 16:

(a) deliberate omission, concealment, or falsification of relevant facts from any personnel security questionnaire, personal history statement, or similar form used to conduct investigations, determine employment qualifications, award benefits or status, determine security clearance eligibility or trustworthiness, or award fiduciary responsibilities; and

(b) deliberately providing false or misleading information concerning relevant facts to an employer, investigator, security official, competent medical authority, or other official government representative.

Applicant acknowledged that he did not disclose all of his security infractions on the April 2013 SCA, but denied that he intentionally attempted to deceive the Government. When a falsification allegation is controverted or denied, as in this case, the Government has the burden of proving it. Proof of an omission, standing alone, does not establish or prove an applicant's state of mind when the omission occurred. An administrative judge must consider the record evidence as a whole to determine whether there is direct or circumstantial evidence concerning an applicant's state of mind at the time the omission occurred. *See* ISCR Case No. 03-09483 at 4 (App. Bd. Nov. 17, 2004) (explaining holding in ISCR Case No. 02-23133 at 5 (App. Bd. Jun. 9, 2004)).

Applicant's explanation for not disclosing all of his security infractions in the April 2013 SCA is credible. He assumed that the Government gained knowledge of his security infractions after they were entered into his employer's database, which he believed was interconnected to the Government's security clearance database. While his assumption was incorrect, it was not unreasonable. Because he was uncertain if the two infractions occurring in December 2012 and February 2013, had reached the Government's database, he disclosed them in his April 2013 SCA. Based on his assumption, he acknowledged that he should have disclosed both February 2013 infractions, including the piece of paper issue. He now also clearly understands that in the future he must disclose all adverse information, as his employer's database does not connect to the Government's database.

The fact that Appellant disclosed all nine infractions to his employer lends sufficient credence to his explanation and state of mind that he did not intentionally falsify his security clearance application or attempt to deceive an investigator during an interview. After listening to Applicant testimony and observing his demeanor, I find that his explanations for failing to disclose specific information, as alleged in SOR ¶ 2, are persuasive and credible. SOR ¶¶ 2(a) and 2(b) are found in his favor. As a consequence, a discussion of the applicability of mitigating conditions is not warranted.

Whole Person Concept

Under the whole person concept, the administrative judge must evaluate an applicant's eligibility for a security clearance by considering the totality of the applicant's conduct and all relevant circumstances. The administrative judge should consider the nine adjudicative process factors listed at AG ¶ 2(a). They include the following:

> (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.

According to AG ¶ 2(c), the ultimate determination of whether to grant eligibility for a security clearance must include an overall commonsense judgment based upon careful consideration of the guidelines and the whole-person concept.

I considered the potentially disqualifying and mitigating conditions in light of all relevant facts and circumstances surrounding this case, including the fact that classified information and the national security were never compromised. Applicant is an educated 58-year-old man, who has dedicatedly worked for a defense contractor since 1980 and held a security clearance during that time. He also has had access to classified networks for many years. Between November 2009 and February 2013, he committed security infractions nine times, eight of which involved accidentally taking his cell phone or laptop into a secured workspace. The ninth incident involved writing unclassified notes on a piece of paper that was located in the secured area, which he took home and promptly returned when he realized his mistake. He received warnings after each incident, and also a corrective action memo and lost a day's pay.

Despite these incidents, Applicant's employer has complete confidence in his ability to comply with security procedures and strongly recommends that he retain his security clearance. His security manager confirmed that the corrective steps Applicant has taken to prevent similar infractions are effective and have eliminated similar incidents. All character references attest to his honesty, ethics, and commitment to security protocols, as evidenced by his self-reporting after each incident. Given Applicant's awareness that a future infraction could result in adverse action, it is unlikely that similar incidents will recur or that Applicant will pose a security risk. Overall, the record evidence leaves me without questions or doubts as to Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude Applicant mitigated the security concerns arising under Guideline K and Guideline E.

Formal Findings

Formal findings for or against Applicant on the allegations set forth in the SOR, as required by section E3.1.25 of Enclosure 3 of the Directive, are:

Paragraph 1, Guideline K:	FOR APPLICANT
Subparagraphs 1.a through 1.i:	For Applicant
Paragraph 2, Guideline E:	FOR APPLICANT
Subparagraphs 2.a and 2.b:	For Applicant

Conclusion

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

_____
SHARI DAM
Administrative Judge