**DEPARTMENT OF DEFENSE**
**DEFENSE OFFICE OF HEARINGS AND APPEALS**

| | | |
|---|---|---|
| In the matter of: | ) | |
| | ) | |
| REDACTED | ) | ISCR Case No. 18-01812 |
| | ) | |
| Applicant for Security Clearance | ) | |

## Appearances

For Government: Andre M. Gregorian, Esq., Department Counsel
For Applicant: *Pro se*

07/16/2019

_____

## Decision

_____

MATCHINSKI, Elizabeth M., Administrative Judge:

While serving as custodian for a high volume of communications security (COMSEC) material, Applicant neglected to secure a safe in the COMSEC room, a stand-alone closed area, in March 2017. Sometime after February 2015, he lost a classified Secret controlled cryptographic item that was within his accountability. He did not report the item as missing for some two years because he believed it would be found. He has a positive attitude toward the discharge of his security responsibilities, and he has shown that he can handle classified information appropriately. Clearance is granted.

## Statement of the Case

On October 3, 2018, the Department of Defense Consolidated Adjudications Facility (DOD CAF) issued a Statement of Reasons (SOR) to Applicant, detailing the security concerns under Guideline K, handling protected information, and explaining why it was unable to find it clearly consistent with the national interest to grant or continue his access to classified information. The DOD CAF took the action under Executive Order (EO) 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 *National Security Adjudicative Guidelines for Determining Eligibility for Access to Classified Information or Eligibility to Hold a Sensitive Position* (AG) effective within the DOD on June 8, 2017.

On November 8, 2018, Applicant answered the SOR allegations and requested a hearing before an administrative judge from the Defense Office of Hearings and Appeals (DOHA). On April 9, 2019, the case was assigned to me to conduct a hearing to determine whether it is clearly consistent with the national interest to grant or continue a security clearance for Applicant. On April 15, 2019, I scheduled a hearing for May 8, 2019.

I convened the hearing as scheduled. Before the introduction of any evidence, the Government moved to amend the SOR under ¶ E3.1.17 of the Directive. Applicant had no objection, and I granted the motion, as set forth below. Six Government exhibits (GEs 1-6) were admitted in evidence, which included as GE 4 an administrative inquiry into a failure by Applicant to secure a Secret GSA container (classified safe) within a COMSEC closed area in March 2017. A December 31, 2018 letter forwarding the proposed GEs to Applicant, and a list of the GEs, were marked as hearing exhibits (HEs I-II) for the record but not admitted in evidence. Nine Applicant exhibits (AEs A-I) were admitted in evidence without any objections. Applicant, his former supervisor, and his current supervisor testified, as reflected in a transcript (Tr.) received by DOHA on June 3, 2019.

## Procedural Ruling

On the Government's motion and with no objections from Applicant, the allegations of the SOR were amended to read as follows:

> a. In about August 2017, while employed with [company name and location omitted], you lost a Secret classified accountable item.
>
> b. In about March 2017, while employed with [company name and location omitted] you left a classified container unsecured within a Secret closed area.

## Findings of Fact

After considering the pleadings, exhibits, and transcript, I make the following findings of fact.

Applicant is a 61-year-old married father with two adult children. He has worked for his defense-contractor employer since August 1983. In 2010, he assumed the duties of alternate COMSEC custodian for the engineering department at his facility, and he transitioned into the role of lead COMSEC custodian by 2014. Applicant held a Secret clearance from November 1993 until June 2010, when it was upgraded to Top Secret.

That clearance was renewed most recently in April 2015. (GEs 1, 3; AEs E-F, H; Tr. 52-54.) He works in a building where all employees are required to possess a minimum of a DOD Secret clearance (Tr. 39, 55, 67), and he has had security training on an annual basis over the years. (Tr. 55-56.)

Applicant had an unblemished record for any security infractions before he took on COMSEC custodian duties at the request of his then supervisor. (Tr. 69, 73.) The supervisor considered Applicant the best candidate because of his reputation, his administrative skills, and his integrity. (Tr. 74.) While leaving work one day in late August 2013, Applicant failed to spin an X-09 lock on the door to a stand-alone COMSEC closed area that housed COMSEC equipment for multiple satellite communications programs. Then the alternate COMSEC custodian at his facility, he was distracted by other duties as he conducted end-of-the-day security checks. Approximately 15 minutes after he left work, an information security systems (ISS) employee discovered that the door to the room was shut, but was not properly secured in that the lock had not been spun. A co-worker with appropriate access to the COMSEC area secured the room, and the ISS employee contacted Applicant, who returned to work and visually inspected the area. He determined that there had been no attempt at unauthorized access. Applicant and his supervisor reported the incident to his facility security officer (FSO) the next day. The facility's FSO conducted an administrative inquiry into the incident and determined that no compromise of classified information had occurred. Under the company's security procedures, a written report of the violation was issued for the "administrative" violation. Applicant was reminded of the proper procedures for securing closed areas and of the company's security policy providing for disciplinary action of up to a five-day suspension for any additional violation within a 12-month period. (GEs 2-3, 6; Tr. 47, 56-57, 68.)

The number of programs requiring COMSEC support increased significantly starting in 2014. (Tr. 66.) As lead COMSEC custodian, Applicant had the difficult task of working through a new electronic keying system. He managed 12 classified COMSEC safes secured by X-09 locks and handled all the crypto-security for two separate facilities for his employer while mentoring a new alternate COMSEC custodian. (Tr. 43-45.) He worked long hours, including some weekends, to ensure that programs met their schedules. He presided over government audits with "No Findings." (AEs E-F.) Applicant's annual performance evaluation for 2015 shows that he had earned the respect of his supervisor and peers. Applicant's supervisor indicated that Applicant had done "a great job handling the ever changing requirements for COMSEC." He gave Applicant an overall rating of "exceeds requirements." (AE E.)

Applicant continued to do an "outstanding job" as COMSEC custodian in 2016. In evaluating Applicant's performance for 2016, Applicant's supervisor remarked that Applicant took his job very seriously, worked well with others, and had become their expert "on the generation, architect, and maintaining of all COMSEC hardware and keys." Time and time again, Applicant worked tirelessly to meet the demands of all the engineers and their programs. (AE D.)

In March 2017, Applicant left a GSA-approved container in the COMSEC room unattended and unsecured for about 15 minutes. The safe was approved for storage of Secret information and contained classified COMSEC equipment and combinations. It was one of seven containers approved for storage of classified COMSEC material located within the COMSEC closed area. Access to the COMSEC closed area was restricted to three individuals with the combination and swipe access. The COMSEC area was inside another approved DOD Secret closed area where Applicant was assisting some engineers. The violation was discovered by a company industrial security employee while conducting a security self-inspection. When questioned by his FSO about his procedures that morning, Applicant acknowledged that he had departed the COMSEC room to assist some engineers within the larger closed area without securing the safe "because he believed that since the container was located inside an approved closed area no action needed to occur." (GE 4.) Applicant now does not recall telling the FSO that he did not need to secure the safe because he knew the proper procedure to secure the classified container was by spinning the X-09 locks. (Tr. 58-59.) He attributes his security infraction to "a lot going on that day." (Tr. 68.) The FSO conducted an internal administrative inquiry into the incident. She concluded that no loss, compromise, or suspected compromise of classified information was presumed because no unauthorized individuals had been present, and no suspicious activity had occurred during the 15 minutes that the safe was unsecured and unattended. Applicant was issued a written warning and required to attend a closed-area security briefing where he was re-educated on the requirements for safeguarding classified information. (GEs 2, 4, 6; Tr. 59-60.) The incident was reported to the DOD CAF by Applicant's employer. (GE 2.)

In April 2017, Applicant informed his then supervisor that he could no longer handle the stress of being the COMSEC manager, given the volume of COMSEC material and having only one other employee, the alternate COMSEC manager, to assist him. After an internal audit by a COMSEC specialist from another facility, who questioned why COMSEC responsibilities were being handled by the engineering department when accounting for COMSEC was a security function in the company's other facilities, Applicant's employer decided to transfer COMSEC responsibilities from the engineering department to the security department, and to increase the staff handling COMSEC duties. (Tr. 40-42, 64, 72.) It took the company several months to assign a COMSEC manager, and a few more months to hire two more COMSEC employees before Applicant was relieved of his COMSEC responsibilities. (Tr. 83-84.)

In September 2017, Applicant informed his FSO that he could not locate a Secret-controlled cryptographic item that was within his accountability. He had recently conducted an inventory of approximately 1,300 items of COMSEC material in August 2017, in preparation for an audit by a U.S. government agency, and was unable to account for an item from a high-volume COMSEC account. During an investigation into the violation by company security personnel, it was discovered that the item had not been sighted during any of four previous semi-annual inventories that had been signed off by Applicant and the alternate COMSEC custodian. Applicant was required to physically touch all pieces of COMSEC hardware during semi-annual inventories. (Tr.

42.) He knew that the Secret cryptographic item had last been seen in February 2015. (GEs 2, 5-6; AE C; Tr. 61-62.) However, he continued to believe that the item was somewhere in the COMSEC room because he had a receipt indicating that it had been returned to COMSEC accountability. (GEs 2, 5; Tr. 49.) He was determined to find the piece of equipment, which was about one square inch in size and part of a "split encryption key" that requires mating to the second half of the key to load operational software. As part of a unique electronic system, it alone is useless in revealing any classified information. (Tr. 50-51.) He did not want to be the first employee to lose a classified item at his worksite, and so he continued to search for the item without success. (Tr. 51.) Applicant was verbally reprimanded by his supervisor, but he was not otherwise disciplined for the violation. (GE 6, Tr. 63, 92.) In reporting the incident to the DOD CAF in late September 2017, Applicant's employer indicated that Applicant was in the process of being removed as the COMSEC custodian because the COMSEC organization was being transitioned to a function of the security department. (GE 2.)

On October 25, 2017, Applicant completed and certified to the accuracy of a Questionnaire for National Security Positions (SF 86). In response to an inquiry concerning whether he had received a written warning, or been officially reprimanded or disciplined for misconduct in the workplace, such as a security violation, in the last seven years, Applicant indicated that he had been disciplined or warned in May 2017 for "1) Security violation (unsecure container) [and] 2) COMSEC account (missing an accountable item)." (GE 1.)

Following the transition of COMSEC custodian responsibilities to the facility's security department in December 2017, Applicant began training to assume a position as a logistics planner. In evaluating Applicant's job performance for 2017, his now former supervisor indicated that the engineering team, program office, and management are indebted to Applicant for all the late nights and weekends he spent as COMSEC custodian to ensure the success of programs. (AE C.) The supervisor made no mention of the security infractions in Applicant's performance evaluation. He discussed the incidents with Applicant, who realized his mistakes, and the supervisor "knew that it wasn't going to be a systemic problem." (Tr. 91.) In January 2018, Applicant filled in for the facility's COMSEC team with no adverse incidents while the team received training offsite. (AE B; Tr. 104.)

On February 5, 2018, Applicant was interviewed by an authorized investigator for the Office of Personnel Management about the two security violations in 2017. He attributed his failure to spin the lock on a classified container to being in a hurry. Concerning the loss of a Secret accountable item, Applicant admitted that he did not immediately report that an item was missing because he thought it would be irresponsible of him to report the loss before he had an opportunity to look for it. He expressed his belief that it was lost during an NSA audit in August 2017 (GE 6), although he now admits that he knew it was missing for some two years. (Tr. 62.) He explained that it was a small item, approximately the size of a USB plug, and so could have slipped through a crack. Applicant indicated that he did not lose his clearance or

his access, and he did not receive a written reprimand. Applicant did not recall any other security violations. (GE 6.)

On April 25, 2018, Applicant was re-interviewed by the OPM investigator and confronted with the details of his August 2013 violation regarding his failure to spin the X-09 lock at the end of the day. Applicant attributed the security infraction to being in a rush and distracted by work demands. Applicant explained that he no longer had COMSEC custodian duties as of February 2018, and he now feels more comfortable and less stressed with his current level of responsibility for classified information. (GE 6.)

In his current position, Applicant no longer has any access to any containers approved for classified storage. He no longer works in the COMSEC storage room and does not have regular access to classified information. (Tr. 69.) His current job function requires that he maintain a Secret clearance. (Tr. 101.) He understands the concern about the failure to timely report the missing COMSEC item and acknowledges that he should have reported it when he first could not find it. (Tr. 108.)

**Character references**

Applicant's supervisor from 1999 through 2017 testified for Applicant and also provided a character reference letter. (AE H.) This supervisor retired from the company in August 2018, after 41 years of service for the company. (Tr. 71.) Throughout their more than 30 years as co-workers, Applicant has been a reliable and trustworthy employee. Applicant's former supervisor attests that Applicant was promoted to COMSEC custodian in 2014 because of his consistent high level of performance as alternate COMSEC custodian starting in 2010. While holding COMSEC custodian responsibilities, the company had several audits by their U.S. government customers and by internal company security personnel, all with favorable results. Applicant's former supervisor considers Applicant to be one of the most security conscious people he has known. (AE H.) At Applicant's hearing the supervisor testified that the COMSEC room was a "very, very stressful area." (Tr. 75-76, 86.) Twelve different programs were "constantly under the gun, as far as time constraints and getting the work done to meet the obligations of the contract[s]" (Tr. 76), and the COMSEC area was understaffed. (Tr. 81.) Regarding the transition of the COMSEC functions to the security department, the supervisor explained that their employer had an internal audit from a COMSEC specialist from another of the company's facilities, who questioned why engineering was in charge of COMSEC responsibilities. (Tr. 80-81.) He added that the company wanted Applicant to retain COMSEC duties as part of the security department. Applicant elected to move to engineering support. (Tr. 82.) In the supervisor's experience, Applicant took his accountability and security responsibilities very seriously. (Tr. 87.) The supervisor believes the violations in 2017 occurred because of Applicant's "tremendous" workload. The security infractions did not shake his confidence in Applicant's ability to protect classified information. (Tr. 88-89.) He blames himself for not paying more attention to the work demands placed on Applicant as COMSEC custodian. (Tr. 86.)

Applicant's current supervisor has worked for the defense contractor for some 34 years. He transferred to Applicant's worksite 21 years ago and has known him since that time. He was one of 12 test directors in their secure building. They "heavily taxed" Applicant in the COMSEC room to maintain their programs. (Tr. 96-97.) Applicant's current supervisor knows of no one he would trust more with national security information than Applicant, who has shown him "nothing but respect, tremendous care, responsibility and [met] all of the, you know, proper traits of just a terrific employee." (Tr. 99.) Applicant's current supervisor corroborated the significant increase in COMSEC work between 2014 and 2017, as the company doubled the number of large programs from 6 to 12 during that time. He considers it responsible of Applicant to have approached his then supervisor in 2017 and told him that the job was "just too stressful." (Tr. 100.) Applicant's current supervisor is aware of Applicant's security violations in 2017. He has confidence in Applicant's ability to handle classified information. (Tr. 102.)

A co-worker, who has known Applicant for some 25 years, respects Applicant for the seriousness and attention to detail he brings to his work. He described Applicant as a "model employee," who leads by example. (AE G.)

Another co-worker, who interacted with Applicant on a daily basis during Applicant's tenure as chief COMSEC custodian at their test site, knows Applicant as a golf partner outside of work. He has always found Applicant to have strong family values and to be "a very upright, honest, and affable person." (AE I.)

In December 2018, Applicant was recognized by his peers and leadership for his outstanding technical contributions in 2018. He was promoted, his official title was changed to include "With Honors," and he was given a $1,500 cash award by his employer. (AE A; Tr. 99.) In evaluating Applicant's annual performance for 2018 in March 2019, Applicant's current supervisor described Applicant's work ethic and commitment to the job as "second to none." Applicant was thorough and competent in taking on new roles, and he took complete ownership of his tasks. (AE B.)

## Policies

The U.S. Supreme Court has recognized the substantial discretion the Executive Branch has in regulating access to information pertaining to national security, emphasizing that "no one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988). When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the adjudicative guidelines. In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially disqualifying conditions and mitigating conditions, which are required to be considered 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 the adjudicative process. The administrative judge's overall 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. Under Directive ¶ E3.1.14, the Government must present evidence to establish controverted facts alleged in the SOR. Under Directive ¶ E3.1.15, the applicant is responsible for presenting "witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by applicant or proven by Department Counsel. . . ." The applicant has the ultimate burden of persuasion to obtain a favorable security decision.

A person who seeks access to classified information enters 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 that the applicant may deliberately or inadvertently fail to 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. Section 7 of Executive Order 10865 provides that 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." *See also* EO 12968, Section 3.1(b) (listing multiple prerequisites for access to classified or sensitive information).

## Analysis

### Guideline K, Handling Protected Information

The security concern for handling protected information is articulated in AG ¶ 33:

> Deliberate or negligent failure to comply with rules and regulations for handling protected information—which includes classified and other sensitive government information, and proprietary information—raises doubt about an individual's trustworthiness, judgment, reliability, or willingness and ability to safeguard such information, and is a serious security concern.

The evidence establishes that Applicant committed three security violations while in the demanding jobs of alternate COMSEC custodian and then COMSEC custodian. When leaving work one day in August 2013, Applicant inadvertently failed to spin an X-09 cypher lock on the door to a COMSEC closed area approved for the storage of classified COMSEC information and equipment. Under ¶ 5-306 of the *National Industrial*

*Security Program Operating Manual* (NISPOM), DOD 5220.22-M, dated February 2006, access to closed areas approved for classified storage must be controlled to preclude unauthorized access. During non-working hours and during working hours when the area is unattended, admittance to the area is required to be controlled by locked entrances and exits, secured either by an approved built-in combination lock, or an approved combination or key-operated padlock. This August 2013 security violation was not alleged in the SOR and so it cannot be considered for disqualifying purposes. In ISCR Case No. 03-20327 at 4 (App. Bd. Oct. 26, 2006), the Appeal Board listed five circumstances in which conduct not alleged in a SOR may be considered, as follows:

> (a) to assess an applicant's credibility; (b) to evaluate an applicant's evidence of extenuation, mitigation, or changed circumstances; (c) to consider whether an applicant has demonstrated successful rehabilitation; (d) to decide whether a particular provision of the Adjudicative Guidelines is applicable; or (e) to provide evidence for the whole-person analysis under Directive Section 6.3.

Applicant's August 2013 security infraction is of little present security concern, given it was inadvertent, and he acted appropriately when informed about his failure to secure the X-09 lock on the COMSEC closed area. He immediately returned to work and made the appropriate checks to ensure that the facility was secured. The next day, he filed a timely report of the August 2013 violation with his FSO. His conduct following the infraction provides evidence of his positive attitude toward his security responsibilities.

In March 2017, Applicant failed to spin an X-09 cypher lock on a safe approved for storage of Secret COMSEC material, after he had been reminded of his obligation to properly secure classified information for the August 2013 incident. Applicant received a written warning for the violation, and he was re-briefed about his security responsibilities in closed areas. His March 2017 security violation (SOR ¶ 1.b) triggers disqualifying condition AG ¶ 34(g), "any failure to comply with rules for the protection of classified or sensitive information." Under ¶ 5-308 of the NISPOM, security containers, vaults, cabinets, and other authorized storage containers are to be kept locked when not under the direct supervision of an authorized person entrusted with the contents.

In August 2017, while conducting an inventory of COMSEC material in preparation for an upcoming audit by the U.S. government, Applicant could not locate a small piece of COMSEC hardware classified Secret that was within his accountability. Applicant violated his responsibility under ¶ 5-100 of the NISPOM, which requires that individuals are responsible for safeguarding classified information entrusted to them. The classified item had last been seen in February 2015. Paragraph 1-303 of the NISPOM states, "Classified material that cannot be located within a reasonable period of time shall be presumed to be lost until an investigation determines otherwise." Applicant's loss of a classified item within his accountability (SOR ¶ 1.a) implicates AG ¶ 34(g) and raises concerns about his security posture under AG ¶ 34(h), "negligence or lax security practices that persist despite counseling by management."

Disqualifying condition AG ¶ 34(i), "failure to comply with rules or regulations that results in damage to the national security, regardless of whether it was deliberate or negligent," has not been established. There is no assessment or conclusion in evidence from the government or from Applicant's employer about whether compromise occurred or cannot be ruled out. Applicant and his former supervisor testified that the missing item is half of a "split key" that has to be mated and then inserted into a unique electronic system to reveal classified information, so should it be found by an unauthorized person, access to classified information would not be easily obtained.

Applicant has the burden of mitigating the security concerns raised by his violations of the rules and regulations for handling protected information. Applicant handled classified information without any problems for some 20 years before he failed to spin the lock on the door to the COMSEC closed area in August 2013. His security violations are very infrequent when considering his many years of holding a DOD clearance without any security violations or infractions. Yet, it is difficult to fully mitigate the security concerns under AG ¶ 35(a). The security violations alleged in the SOR did not occur so long ago. Moreover, although it was alleged that Applicant lost a classified item in August 2017, the evidence shows the classified item had not been seen since February 2015; that Applicant knew it was missing because he had conducted semi-annual inventories since that time; and that he did not report the item as missing to his FSO until September 2017. He failed to comply with security requirements over the course of two years, so it was not an isolated event. AG ¶ 35(a) provides:

> (a) so much time has elapsed since the behavior, or it 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.

Reform is established under AG ¶ 35(b) when "the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities." Regarding Applicant's March 2017 failure to spin the X-09 lock on one of the seven classified safes in the COMSEC room, Applicant left the container unsecured and unattended for about 15 minutes while he assisted some engineers outside of the COMSEC room but in the larger closed area accessed only by authorized personnel with appropriate clearances. He told his FSO that he did not think that he had to secure the security container because it was located inside an approved closed area. However, he admitted at his hearing that he knew that he should have properly secured the container and that it was not his practice to leave the safes unlocked. Applicant has accepted full responsibility for the March 2017 infraction alleged in SOR ¶ 1.b.

Regarding the violation alleged in SOR ¶ 1.a, Applicant's loss of the classified COMSEC item was unintentional, but he did not inform his FSO about the missing item until September 2017. His employer's investigation revealed that the item had not been sighted during any of four previous semi-annual inventories that had been signed off by Applicant as COMSEC custodian and by the alternate COMSEC custodian. About the

semi-annual inventories, Applicant testified that, as COMSEC custodian, he had to physically touch all pieces of COMSEC equipment and report to the government. As a longtime cleared employee, Applicant can be expected to have known about his obligation to timely report the possible loss of a classified item to his FSO under ¶ 1-300 of the NISPOM. His belief that the item would eventually be found cannot justify such a lengthy delay in complying with his reporting obligation. Even so, there is some evidence of reform in that brought the missing item to the attention of his FSO in September 2017, albeit very belatedly. He did not display a cavalier attitude when verbally reprimanded for the violation by his then supervisor. Applicant's former and current supervisors and two longtime co-workers attest to the seriousness with which Applicant has taken security throughout his career. AG ¶ 35(b), "the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities," has some applicability.

Applicant testified that he received annual security training throughout his employment. There is no indication that AG ¶ 35(c), "the security violations were due to improper or inadequate training or unclear instructions," applies. AG ¶ 35(d), "the violation was inadvertent, it was promptly reported, there is no evidence of compromise, and it does not suggest a pattern," is established with regard to the August 2013 and March 2017 violations that involve the failure to properly secure the COMSEC room at the end of the work day and leaving unsecured the classified container in the COMSEC room, respectively. Although the March 2017 violation was found during a security self-inspection by another employee, and not self-reported, it was inadvertent and there was no compromise. Applicant did not set out to lose or misplace the Secret COMSEC item within his accountability, but AG ¶ 35(d) cannot reasonably apply in mitigation of the security violation in SOR ¶ 1.a because Applicant knew that the item had been missing for some two years before he reported it missing.

**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 his conduct and all relevant circumstances in light of the nine adjudicative process factors in AG ¶ 2(d):

> (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.

Some of the adjudicative process factors were addressed under Guideline K, but some warrant additional comment. Applicant was motivated to perform his COMSEC duties to the best of his ability in a very stressful work environment with only the alternate COMSEC custodian to assist him. Applicant was responsible for handling and safeguarding more than 1,000 COMSEC items. It is perhaps not surprising that an item about a square inch in size would "fall between the cracks." Yet the fact that it was half of a split key that would be useless without the other half does not excuse the loss of the classified COMSEC hardware. It certainly does not justify his failure to report for some two years that he could not locate an item within his accountability. When discussing the incident with the OPM investigator in February 2018, Applicant was less than fully forthcoming about when he first realized the item was missing. He indicated that he noticed the item was missing during an inventory for a change of COMSEC custodian in 2017 and that he looked for the item for three weeks before reporting it missing. Applicant now admits that he knew that the item was missing for some two years. While the loss of the classified item was inadvertent, he raised some doubt about whether he can be counted on to timely and candidly report when his conduct falls short of full compliance with his security responsibilities.

The security clearance adjudication involves an evaluation of an applicant's judgment, reliability, and trustworthiness in light of the security guidelines in the Directive. *See* ISCR Case No. 09-02160 (App. Bd. Jun. 21, 2010). It is not designed to punish applicants for past mistakes or shortcomings. There is considerable evidence supporting continuation of a security clearance for Applicant. Applicant's then supervisor blames himself for not paying more attention to the work demands placed on Applicant as COMSEC custodian. He considers Applicant to have been an outstanding COMSEC custodian, even in 2017, despite knowing that Applicant failed to timely report the COMSEC item as missing. He chose not to comment about the presumed loss of the COMSEC item in Applicant's annual performance evaluation for 2017 because he did not see it as a systemic problem. In his opinion, Applicant displayed a serious attitude toward the discharge of his security responsibilities. It is noteworthy that Applicant's employer did not remove Applicant from COMSEC duties or impose discipline beyond a verbal reprimand from his immediate supervisor for the loss of the COMSEC item. Applicant continued to perform COMSEC duties throughout the transition until December 2017, and he filled in for COMSEC employees when they had training in January 2018. Applicant's current supervisor remains confident in Applicant's ability to appropriately handle classified information. Applicant has continued to be a valuable contributor at work, as evidenced by him being recognized by his peers for his technical excellence and leadership in December 2018. Applicant is now in a less demanding position with respect to the risk of mishandling classified information. He understands that he should have timely notified his employer about the missing COMSEC item. After considering his overall security posture since 1993, he does not present an unacceptable security risk going forward. This does not mean that his security violations are condoned, but he has adequately demonstrated that he can be counted on to discharge his security responsibilities in accord with policies and regulations.

## Formal Findings

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

| | |
|---|---|
| Paragraph 1, Guideline K: | FOR APPLICANT |
| Subparagraphs 1.a-1.b: | For Applicant |

## Conclusion

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

_____
Elizabeth M. Matchinski
Administrative Judge