Date: April 26, 2023

| | | |
|---|---|---|
| In the matter of: | ) | |
| ----- | ) | ISCR Case No. 20-01608 |
| Applicant for Security Clearance | ) | |

**APPEAL BOARD DECISION**

**APPEARANCES**

**FOR GOVERNMENT**
James B. Norman, Esq., Chief Department Counsel

**FOR APPLICANT**
***Pro se***

The Department of Defense (DoD) declined to grant Applicant a security clearance. On March 17, 2021, DoD issued a statement of reasons (SOR) advising Applicant of the basis for that decision—security concerns raised under Guideline K (Handling Protected Information) and Guideline E (Personal Conduct) of Department of Defense Directive 5220.6 (Jan. 2, 1992, as amended) (Directive). Applicant requested a hearing. On February 28, 2023, after the hearing, Defense Office of Hearings and Appeals (DOHA) Administrative Judge Matthew E. Malone denied Applicant's request for a security clearance. Applicant appealed pursuant to Directive ¶¶ E3.1.28 and E3.1.30.

Under Guideline K, the SOR alleged 10 security concerns, including two failures to secure classified documents properly, five instances of bringing her cellphone into a secure facility, and three instances of failure to report her cellphone violations. That same conduct was cross-alleged under Guideline E. The Judge found adversely to Applicant on all Guideline K allegations and favorably to Applicant on the Guideline E allegation.

Applicant raised the following issues on appeal: whether the Judge failed to consider all available evidence and misapplied the mitigating conditions, rendering his adverse decision arbitrary, capricious, or contrary to law. Consistent with the following, we affirm.

**The Judge's Findings of Fact:** The Judge's findings are summarized in pertinent part.

Applicant is in her early fifties and married. She holds a bachelor's and master's degree. With the exception of a three-year break between 2011 and 2014, Applicant has worked for her defense contractor employer since 1995.

In 2015, Applicant's company was awarded a number of new classified projects and rapidly expanded both its workforce and its use of Sensitive Compartmented Information Facilities (SCIFs) and Special Access Program Facilities (SAPFs). Although she had previously held a security clearance, Applicant had not previously worked in SCIFs or with classified information. During this period of growth and transition to working in SCIFs, employees were briefed on security requirements for working in secure spaces, including the prohibition against bringing cellphones into SCIFs.

Between September 2015 and January 2017, Applicant entered a SCIF with a cellphone on her person on five occasions. Each incident was inadvertent, discovered quickly, and promptly remedied by securing the cellphone in a locker. In the first two instances of September 2015 and May 2016, Applicant timely reported the infractions. In both incidents, the security office examined the cellphone, confirmed that there was no compromise, and counseled Applicant about the no-cellphone rule. After the second incident, Applicant no longer brought her company cellphone into the building, but she continued to bring her personal phone.

Applicant inadvertently entered a SCIF with her personal cellphone in her purse or pocket on three more occasions—in June 2016, July 2016, and early January 2017. Each time, she quickly discovered the cellphone and removed it, but she failed to report the incidents promptly as required. In mid-January 2017, Applicant attended security refresher training that reinforced the need to self-report any security violations or infractions, and she reported all three events. The employer's subsequent investigation determined that, although each individual event constituted a security infraction, the total of five cellphone incidents and her failure to report three of them rose to the level of a security violation.

Applicant received a letter of reprimand after the January 2017 security office investigation, as well as informal counseling by security staff. Applicant took remedial actions that included forwarding her personal cellphone calls to her office desk phone, leaving her cellphone in her car, and requesting a pager that could be taken into the SCIF. The record does not indicate that she received any remedial security training following her violation. In 2018, the company renovated the work spaces and required employees to relinquish their cellphones upon first entering the building to reduce the incidences of cellphones being brought into the SCIFs.

In addition to her cellphone violations, Applicant mishandled classified information on two occasions. Although her desk was in a secure space, that space was not approved for open storage, and the documents were required to be secured in an approved safe or other locked container. In June 2018, Applicant reported to security that she had inadvertently left a classified PowerPoint presentation on her desk overnight.

In January 2019, Applicant again reported to security that she had inadvertently left a classified document on her desk overnight. The document had been handed to her by a co-worker,

and Applicant had not initially recognized it to be classified, in part due to the co-worker's admitted failure to package the document appropriately. Upon recognizing the following day that the document was marked classified, Applicant reported the matter to security.

In both instances, the security office determined the infractions to be the result of Applicant's negligence with no risk of compromise. Applicant testified she received a letter of reprimand that addressed both her June 2018 and January 2019 infractions. After the latter incident, Applicant devised a checklist to use at the end of every workday to ensure nothing in her area of responsibility was left unsecured. Applicant also testified concerning incidents in which she either reported security violations of others or brought violations to the offenders' attention and encouraged them to self-report.

Applicant presented information suggesting that her employer's security practices were deficient, specifically that training was insufficient because there was no special attention paid to cellphone infractions and that she received no remedial training after the incidents. However, the security office's records indicate that Applicant was verbally counseled about the rule against cellphones after each reported incident, and she stated multiple times that she understood the rules.

In responding to the SOR, Applicant disclosed another instance in which she brought her company cellphone into a secure space. Although not alleged in the SOR, this event was explored at the hearing and was considered on the issue of mitigation. In January 2017, Applicant completely deactivated her company cellphone after receiving a pager. Although she was instructed to mail the cellphone to a corporate facility for disposal, Applicant forgot to do so. In 2019, Applicant brought breakfast to her team in a secure space, as they were working on a weekend. She used her travel bag from the car to transport the food and subsequently discovered that the deactivated cellphone was still in the bag. It was not charged and appeared to be inoperable even if charged. Shortly thereafter, Applicant mailed the device for disposal. Applicant did not report the matter to her employer because the device was inoperable and because she was wary of the consequences in light of her letter of reprimand from January 2017.

Applicant has an exemplary performance record. A former supervisor testified on her behalf and her current supervisor submitted a letter of support. Her performance review, letters of recommendation, and community involvement reflect positively on her character and reliability.

**The Judge's Analysis:** The Judge's analysis is quoted below in pertinent part.

> Applicant's last reported violation occurred in January 2019. As to her improper handling of documents in 2018 and 2019, they were infrequent, and she is unlikely to repeat those infractions after receiving a second letter of reprimand and since devising a checklist to use at the end of every workday. As to her cellphone violations, the last infraction occurred five years ago, and she is unlikely to repeat them because she uses an approved pager instead of a cellphone. Even though she became busy starting in 2015 and may not have been sensitive to the no-cellphone rule before her first infraction, they persisted despite the fact she was counseled about this simple rule each time she self-reported her actions. Although she was aware of the significance of violating this rule, she decided three times to

not self-report because of concerns about the consequences that might result. Not only did Applicant decide to not self-report, she also has not told her employer about the cellphone she brought into the SCIF in late summer or early fall of 2019. She believes doing so would serve no useful purpose and because she, again, was concerned about the consequences. The phone may, indeed, be of no consequence; however, that is not her determination to make.

. . .

Applicant . . . cites a lack of efficiency and follow through by her employer in ensuring that she was properly trained in proper security procedures. . . . [A]vailable information shows that Applicant knew that she should not bring her phone into a SCIF and that her SCIF was not approved for open storage of classified documents. . . . It is difficult to see how, given Applicant's experience since 2015, how more training would have helped her better understand her obligations regarding cellphone rules, document storage, and most important, self-reporting.

. . .

Each alleged violation or infraction, standing alone, may not be considered a significant event. However, the record as a whole regarding these events presents a more repetitive disregard for security procedures, and it does not support a conclusion that this conduct will not recur. On balance, available information shows that Applicant has not established any of the . . . mitigating conditions. [Decision at 10–12.]

**Discussion**

On appeal, Applicant argues that the Judge failed to consider all the evidence and failed to apply the mitigating conditions properly. In particular, Applicant notes that the Judge acknowledged that she is unlikely to mishandle classified information or commit cellphone violations in the future and that his decision instead relies primarily on her failure to report several of her infractions. Applicant highlights that she did ultimately self-report following annual refresher training: "Characterization that there was no self-reporting is inaccurate and an error as self-reporting this matter was the means in which [a] violation was brought forward[.]" Appeal Brief at 2. Regarding the non-alleged cellphone incident—in which she brought her deactivated company cellphone into the workspace in 2019—Applicant highlights that this matter was revealed "by virtue of my honesty and disclosure of potentially relevant information." *Id*. The Judge's decision, she argues, "inaccurately extends the conclusion from a failure to timely report to a complete failure to report, which is inaccurate." *Id.*

Contrary to Applicant's arguments, however, the Judge's decision clearly reflects that he recognized that Applicant "felt the need to clear her conscience" and reported all three incidents shortly after the January 2017 annual refresher training. Decision at 5. In his analysis, the Judge explicitly references Applicant's failure "to **timely** self-report." *Id*. at 9. (Emphasis added.) Regarding the company cellphone incident disclosed in Applicant's response to the SOR, the

Judge notes that "it is commendable that she disclosed that incident as part of this proceeding[.]" *Id*. at 11. In sum, the Judge clearly considered those facts that Applicant represents he overlooked.

As the Judge noted, "access to classified information imposes a fiduciary obligation[.]" Decision at 13. Once it is established that an applicant has engaged in conduct that has negative security implications, the applicant has a heavy burden of persuasion that it is clearly consistent with the national interest to grant or continue a security clearance. Because security violations strike at the heart of the industrial security program, an administrative judge must strictly scrutinize any claims of reform and rehabilitation. *See, e.g.*, ISCR Case No. 00-0030 at 9 (App. Bd. Sep. 20, 2001).

Applicant notes that the Judge erred in some of his factual findings (*e.g.*, his characterization of her workspace as a SCIF rather than a SAPF), but Applicant concedes that the errors are comparatively *de minimis*. We agree—the errors cited are harmless as they did not likely have an impact on the outcome of the case. *See, e.g.*, ISCR Case No. 00-0104 at 3 (App. Bd. Mar. 21, 2001).

None of Applicant's arguments are enough to rebut the presumption that the Judge considered all of the record evidence or to demonstrate the Judge weighed the evidence in a manner that was arbitrary, capricious, or contrary to law. Moreover, the Judge complied with the requirements of the Directive in his whole-person analysis by considering all evidence of record in reaching his decision. *See, e.g.*, ISCR Case No. 19-01400 at 2 (App. Bd. Jun. 3, 2020).

Applicant failed to establish that the Judge committed any harmful error or that she should be granted any relief on appeal. The Judge examined the relevant evidence and articulated a satisfactory explanation for the decision. The decision is sustainable on the record. "The general standard is that a clearance may be granted only when 'clearly consistent with national security.'" *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988). *See also*, Directive, Encl. 2, App. A ¶ 2(b): "Any doubt concerning personnel being considered for national security eligibility will be resolved in favor of the national security."

## Order

The decision is **AFFIRMED**.

Signed: James F. Duffy
James F. Duffy
Administrative Judge
Chair, Appeal Board

Signed: Moira Modzelewski
Moira Modzelewski
Administrative Judge
Member, Appeal Board

Signed: Gregg A. Cervi
Gregg A. Cervi
Administrative Judge
Member, Appeal Board