DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	
[NAME REDACTED]	)	ISCR Case No. 20-01608
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: John C. Lynch, Esq., Department Counsel
For Applicant: Jeffrey D. Billett, Esq.

02/28/2023

_____

Decision

_____

MALONE, Matthew E., Administrative Judge:

Security concerns about Applicant's multiple security violations remain unresolved. Her request for continued eligibility for access to classified information is denied.

Statement of the Case

Applicant has held a security clearance as required by her employment at the secret and top-secret levels since 1995. On March 13, 2019, she submitted an Electronic Questionnaire for Investigations Processing (e-QIP) to renew her clearance eligibility for a security clearance. Based on the results of the ensuing background investigation, Department of Defense (DOD) adjudicators could not determine, as required by Security Executive Agent Directive (SEAD) 4, Section E.4, and by DOD Directive 5220.6, as amended (Directive), Section 4.2, that it is clearly consistent with the interests of national security for Applicant to have a security clearance.

On March 17, 2021, DOD issued to Applicant a Statement of Reasons (SOR) alleging facts that raise security concerns under the adjudicative guidelines for handling protected information (Guideline K) and for personal conduct (Guideline E). The guidelines cited in the SOR were part of the current set of adjudicative guidelines (AG) issued by the Director of National Intelligence on December 10, 2016, to be effective for all adjudications on or after June 8, 2017.

Applicant timely responded to the SOR (Answer) and requested a hearing before an administrative judge at the Defense Office of Hearings and Appeals (DOHA). I received the case on June 9, 2022. On September 29, 2022, I convened the requested hearing using a video teleconferencing platform. The parties appeared as scheduled. I received a transcript of the hearing (Tr.) on October 21, 2022.

With her Answer, Applicant included documents identified as Applicant's Exhibits (AX) A through D. At hearing, Applicant proffered additional documents to be included with AX A and AX B. AX A – D remained part of the record as attached to the Answer and were admitted without objection as evidence along with the additions proffered at hearing. (Tr. 15 – 18) Additionally, Applicant and another witness testified. DOHA Department Counsel proffered Government Exhibits (GX) 1 – 3, which were admitted without objection. (Tr. 13 – 14)

Findings of Fact

Under Guideline K, the Government alleged that in January 2019, Applicant failed to properly secure a marked, classified document in an approved container overnight (SOR 1.a); and that in June 2018, Applicant failed to properly secure a marked, classified document in an approved container overnight (SOR 1.b). It also alleged that in January 2017 (SOR 1.c), July 2016 (SOR 1.d), June 2016 (SOR 1.e), May 2016 (SOR 1.f), and September 2015 (SOR 1.g), Applicant brough her personal cellphone, a prohibited device, into a secure facility at her work location. Finally, the SOR alleged that Applicant did not follow required self-reporting procedures after the January 2017 (SOR 1.h), July 2016 (SOR 1.i), and June 2016 (SOR 1.j) cellphone incidents. Under Guideline E, the Government cross-alleged as adverse personal conduct, the information presented under SOR 1.a – 1.j (SOR 2.a).

In her response, Applicant admitted, with explanations and supporting documents, all the Guideline K and E allegations. (Answer) In addition to the facts established by her admissions, I make the following findings of relevant fact.

Applicant is a 52-year-old employee of a defense contractor. She and her husband have been married since June 1997. She holds a bachelor's and master's degrees earned in 1994 and 2002, respectively. She has worked for her employer since 1995, first as a contracted employee, then as a direct hire. In March 2011, her husband took a job in another state and Applicant left her job to move with him. When they returned in June 2014, Applicant resumed working for her current employer. (Answer; GX 1)

From the time she started working for her employer in 1995 until 2015, the offices and other facilities in which Applicant worked were generally not secured, such as a Secure Compartmented Information Facility (SCIF) or a Special Access Program Facility (SAPF). SAPFs are usually located within SCIFs. Classified work in those facilities is regulated by specific rules regarding access, internal storage of documents, and use of electronic devices, such as cellphones, laptops, and tablets. Although Applicant has held a security clearance during the entirety of her employment, it was not until September 2016 that she began working primarily with classified information and in a SCIF fulltime. Additionally, starting in 2015, Applicant's company experienced a rapid expansion of its workforce for newly awarded classified projects, for which an increased use of SCIFs became necessary. Applicant was assigned as a manager for both the substantive work on one of those projects and for hiring and oversight of new personnel in her part of the organization. Before 2015, she was responsible for 15 personnel. After 2015, she eventually was tasked with oversight of between 70 and 140 personnel. This resulted in a sharp uptick in her workload under often stressful conditions. She was issued a company cellphone and laptop, and had to travel to other job sites on a regular basis. In short, Applicant became a very busy person. (Answer; Tr. 23 – 25, 26 – 30, 122 – 123)

As part of this rapid expansion, and in addition to basic security procedures required of all persons holding clearances, employees were briefed on security requirements for working in secure spaces. A common subject of those briefings, held at least annually, was the rule against bringing cellphones, both personal and work-issued, into SCIFs. Those secure spaces were located within a larger building for which entry and mobility were not as restrictive as for inside the secured areas. Lockers were installed next to the entrance of each SCIF so that employees could secure their cellphones and other prohibited devices on the way into those spaces. Because of the ubiquitous nature of cellphones in society and the workplace, it appears that violating the cellphone prohibition was a common occurrence, so much so that around 2018, the company renovated its workplace to improve the way cellphones were regulated. After the renovation, rather than being able to move about with one's phone in an unclassified area before going into a SCIF, employees were required to relinquish unapproved devices as soon as they entered the building. Signage reflecting the rules about cellphones and other electronic devices was made more prominent, and it appears the number of violations decreased significantly. (Answer; Tr. 78 – 80, 125 – 126)

SOR 1.g: On September 23, 2015, not long after she was assigned as a manager, she attended a meeting in a SCIF with the manager of a team involved in classified work to which some of Applicant's personnel were assigned. She had never been in that SCIF before. She was still carrying both phones in her purse in violation of rules against taking them into a SCIF. During the meeting, one of her cellphones rang. She silenced the phone, secured them both in one of the lockers she had passed on her way into the SCIF, and returned to the meeting. The person with whom she was meeting saw the phones and stated he would not report her, and even suggested a way she could avoid being found to have violated the no cellphone rule. She stated she was not comfortable with

that approach and left the SCIF to properly secure the phones. When the meeting was over, she self-reported her actions to the company security office. Applicant's phones were examined, and she provided information about the incident by completing a "Supplemental Questionnaire – Prohibited Devices." There was no apparent compromise of sensitive information, and the company did not discipline Applicant as a result of her conduct. The security office employee who conducted the investigation of this incident counseled Applicant about the need to properly store her cellphones outside of secure areas. After this incident, Applicant did not change her routine or the way she handled her phones because going to that, or any other SCIF was not yet part of her usual routine. (Answer; GX 2; GX 3; Tr. 25 – 42)

SOR 1.f: On May 2, 2016, before going to her own office, Applicant went to an unclassified part of the building she worked in to begin "onboarding" new employees. At some point, she brought some of them to the security office for in-processing. The security office was in a SCIF, so the new employees waited outside while Applicant went in to begin that part of their check-in process. When she entered the SCIF, she had both of her cellphones in her hand. A security office employee pointed out the phones to Applicant, who said "oops." She then left the space to secure the phones in a locker at the entrance. Having been seen with cellphones in a SCIF by a security staff member, she self-reported the violation, and the matter was dealt with in same manner as her September 2015 violation. Again, no classified information was compromised, no discipline was taken, and Applicant was counseled about the no-cellphone rule by a security staff employee. After this incident, Applicant chose to deactivate the voice functions on her company phone and leave it in her car. The only time she used that phone was for monthly travel, so she had no use for it inside her secure workspaces. Applicant still carried her personal phone to work to stay in touch with her family as needed, and she resolved to be more vigilant about keeping the phone out of SCIFs. (Answer; GX 2; GX 3; Tr. 42 – 48)

SOR 1.e and 1.j: At the beginning of her workday on an unspecified date in June 2016, Applicant walked into the SAPF where her desk was located. When she put her purse on her desk, she noticed one of her cellphones protruding from the bag. She put the phone in her pocket, walked out of the secure area, and stored it in a locker. No one witnessed this incident, and she did not report it when it happened as required. She did not report her conduct because she was afraid of the consequences that might ensue after a third cellphone violation. There is no indication that any sensitive information was compromised. (Answer; GX 2; GX 3; Tr. 48 – 49, 51)

SOR 1.d and 1.i: At lunchtime on an unspecified date in July 2016, Applicant left her secure space and retrieved her personal phone that she had stored in a locker before entering the SCIF. After using the phone to check messages outside the SCIF, she returned directly to the secure area with the phone and a notebook under arm. When she set the notebook down on her desk, she realized she still had her cellphone with her. She left the SCIF and stored the cellphone in a locker as required. Again, no one had witnessed this incident and Applicant did not self-report this event as required. She also

did not make any changes to the way she was handling her personal cellphone. (Answer; GX 2; GX 3; Tr. 49 – 52)

SOR 1.c and 1.h: On January 5, 2017, Applicant left a SCIF during a break in a meeting she was attending there. She retrieved her cellphone from the locker in which she had stored it before the meeting. After checking for messages, she put it in her coat pocket at the same time a co-worker asked to talk with her back in the SCIF for a few minutes. He held the door open for her and she entered without first storing her cellphone in locker. After a brief discussion, she again left the SCIF and realized she still had the phone in her pocket. After going to the restroom, she again secured it in a locker before reentering the SCIF to continue the meeting. No one else knew she had the phone in the SCIF, and she did not report this event as required. Again, she feared the consequences knowing that she had committed multiple cellphone infractions during the prior 18 months. (Answer; GX 2; GX 3; Tr. 52 – 54)

After her January 2017 cellphone incident, Applicant attended a previously scheduled security refresher training on January 16, 2017, that reinforced the need to self-report any security violations or infractions. After that training, she felt the need to clear her conscience about her unreported cellphone infractions in June and July 2016, and in January 2017. She reported all three incidents on January 23, 2017. The company security office processed each of the three events in the same manner as the September 2015 and May 2016 incidents. In assessing the failure to self-report each incident, it was determined that, although each individual event constituted a security infraction, all five events and her failure to report three of them rose to the level of a security violation. The investigation of that violation included a detailed statement from Applicant and a determination by the security staff that she was culpable of a security violation. In findings issued on January 28, 2017, security personnel also recommended that she thereafter be subject to periodic interviews by the security staff "to ensure that she has reported all incidents to the Security office," and that "[m]anagement will provide a summary of selected corrective action(s) to Security within two weeks of receiving this report." According to Applicant, no one interviewed her after that report was issued, and there were no corrective actions identified. (Answer; GX 2; GX 3; Tr. 54 – 56)

Applicant received a letter of reprimand after the January 2017 security office report. The only subsequent corrective action by management consisted of informal counseling by security staff, which included suggesting ways Applicant could change her daily routine to make her more aware of the no-cellphone rule. Applicant herself took actions such as wearing rings in a certain way to sensitize her about what might be in her hands. She also had her cellphone calls forwarded to her office phone so she could leave the cellphone in her car each day. In December 2016, Applicant asked for a pager that could be taken into secure spaces so her family could contact her without using her cellphone; however, Applicant did not receive the pager until after her January 5, 2017, infraction. Available information does not show that she received any remedial security training in response to her violation. (GX 3; Tr. 56 – 60)

SOR 1.b: On June 12, 2018, Applicant reported to security that she had mishandled classified documents by leaving them on her desk overnight. Even though her desk was in a secure space, that space was not approved for open storage. Therefore, the documents were required to be secured in an approved safe or other locking container. The documents were Powerpoint slides intended for display on June 11 in a conference room approved for open storage; however, when she got to the room it was being used, so she returned to her desk, intending to return to the conference room to put the slides up later. Applicant put the slides on her desk but became busy thereafter and forgot about them. She failed to properly store the slides before leaving for the day. She saw them when she returned to work the next morning and reported the matter to security. A subsequent investigation determined this to be an infraction caused by negligence, and that there was no likelihood of compromise. No disciplinary measures resulted from this infraction. (Answer; GX 1; GX 2; GX 3; Tr. 60 – 67)

SOR 1.a: On January 31, 2019, Applicant reported to security that she had mishandled classified documents by leaving them on her desk overnight. Even though her desk was in a secure space, that space was not approved for open storage. Therefore, the documents were required to be secured in an approved safe or other locking container. On January 29, she met with a co-worker who worked in another building. The meeting was held in a secure conference room in Applicant's building. During the meeting, the co-worker handed Applicant a document marked as classified. It was not protected from view by a manila folder as it should have been if the co-worker brought it from another building. After the meeting, Applicant returned to her office and put the document on her desk. It remained there until late the following day, when she noticed for the first time that the document had classified markings on it. She shredded it before leaving for the day and self-reported this incident to security the next morning. Applicant asserts that she did not immediately realize the document had classified markings on it, because they were in black instead of red as required, and as already noted, it had not been carried to the meeting in a manila folder as required. For his part, Applicant's coworker asserted that the document was properly marked, but acknowledged that it was carried improperly (he folded it in half inside a notebook) between buildings. Applicant denies that the document was folded at all. (GX 1; GX 2; GX 3; Tr. 68 – 71)

After Applicant self-reported the January 2019 incident, the security office determined that there was no risk of compromise and that the infraction was the result of Applicant's negligence. Applicant testified she received a letter of reprimand after this incident that also addressed her June 2018 infraction. She claims the letter, which was not produced at hearing, and which she claims her employer has not produced despite her repeated requests, accused her of "unethical" conduct in connection with those events. Applicant takes umbrage with that characterization, which she felt was overly harsh under the circumstances. After this incident, Applicant devised a checklist to use at the end of every workday to ensure nothing in her area of responsibility is left unsecured. A previous version was provided at the hearing as an example of her efforts to avoid similar misplacement of classified information in the future. Applicant also testified that

she has either reported security violations of others or has brought potential security violations to the offenders' attention and encouraged them to self-report. (Answer; GX 1; GX 2; GX 3; AX C; AX D; Tr. 74 – 78)

Applicant presented information suggesting that her employer's security practices were deficient. She argued that her training was insufficient because there was no special attention paid to cellphone infractions, and that in response to her violations, there was no remedial training provided. She did not identify what that training would entail or how any deficient security practices by her employer caused her to commit any of her security infractions. The investigative materials that documented security officials' responses to all her cellphone infractions show that she was verbally counseled about the rule against cellphones each time, and she stated multiple times that she understood the rules. (Answer; GX 3; AX C; Tr. 88 – 94)

In a footnote in Applicant's response to the SOR (Answer at page 5, fn1), she recounted another instance in which she brought a prohibited device – her company cellphone – into a secure space. This conduct was not alleged in the SOR, but was further developed through her hearing testimony, both on direct and cross-examination. (I am only examining it as part of my assessment of information probative of mitigation.) As previously discussed, after her May 2016 cellphone infraction, Applicant decided to deactivate most of the voice functions in her company cellphone and leave it in her car. She then kept the device in a bag she used when she traveled and in which she would also carry her laptop and other business-related travel needs. In January 2017, after she received a pager, she had company technicians completely deactivate the phone. The company then instructed her to send the device to a corporate facility for disposal. In the late summer or early fall of 2019, Applicant and her team were working on a weekend, and she decided to treat her team members to bagels and coffee in the SCIF. To carry the food and drink, as well as the usual items she brought to the office every day, she retrieved the travel bag from her car. Believing it to be empty, she filled it with the items she needed to carry, then entered the SCIF. When she emptied the bag of its contents in the SCIF, she found the deactivated cellphone. She had forgotten to send the device to the corporate facility as she had been instructed to do. The device itself was not charged and appeared to be unusable even if charged. Not long thereafter, she sent the device for disposal. Applicant never reported this incident to the company security staff. She averred that she did not report this matter because it would serve no purpose to report that she had brought a useless device into a SCIF. She also was wary of the consequences of reporting her actions after she had been cited for "unethical" conduct in her second letter of reprimand a few months earlier. While that letter was not produced for this record, the testimony of her former supervisor confirmed the nature of the letter and he response to it. Additionally, Applicant disclosed her receipt of the second letter of reprimand in her most recent e-QIP and it was discussed during her July 15, 2019, personal subject interview (PSI). (Answer; GX 1; GX 2; Tr. 82 – 88, 110 – 111)

Applicant has accrued an exemplary record of performance during her tenure at her company. She also enjoys a solid reputation in the workplace and has been

recognized for her own professional accomplishments and as a mentor to young engineers. In the community, she and her husband are personally vested in specific charities related to their family's experiences and interests stemming from the loss of one of their children. Applicant's former supervisor (he is now retired) testified that he knew her to be an excellent employee and that he would unreservedly recommend her for a position of trust despite his knowledge of some of her security incidents. Applicant's performance reviews, letters of recommendation (including from her current supervisor), various technical qualifications and certifications also reflect positively on her character and reliability. (AX A – C; Tr. 98 – 101, 119 – 123)

Policies

Each security clearance decision must be a fair, impartial, and commonsense determination based on examination of all available relevant and material information, and consideration of the pertinent criteria and adjudication policy in the adjudicative guidelines (AG). (*See* Directive, 6.3) Decisions must also reflect consideration of the factors listed in ¶ 2(d) of the guidelines. Commonly referred to as the "whole-person" concept, those factors are:

> (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.

The presence or absence of a disqualifying or mitigating condition is not determinative of a conclusion for or against an applicant. However, specific applicable guidelines should be followed whenever a case can be measured against them as they represent policy guidance governing the grant or denial of access to classified information. A security clearance decision is intended only to resolve whether it is clearly consistent with the national interest for an applicant to either receive or continue to have access to classified information. (*See* Department of the Navy v. Egan, 484 U.S. 518 (1988))

The Government bears the initial burden of producing admissible information on which it based the preliminary decision to deny or revoke a security clearance for an applicant. Additionally, the Government must be able to prove controverted facts alleged in the SOR. If the Government meets its burden, it then falls to the applicant to refute, extenuate or mitigate the Government's case. Because no one has a "right" to a security clearance, an applicant bears a heavy burden of persuasion. (Egan, 484 U.S. at 528, 531) A person who has access to classified information enters into a fiduciary relationship with the Government based on trust and confidence. Thus, the Government has a

compelling interest in ensuring each applicant possesses the requisite judgment, reliability and trustworthiness of one who will protect the national interests as his or her 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. (Egan at 531; *see* AG ¶ 2(b))

Analysis

Handling Protected Information

Between 2015 and 2019, Applicant committed ten violations of rules intended to safeguard classified information. Information about her conduct in this regard reasonably raises a security concern about her willingness or ability to properly safeguard sensitive information. That security concern is stated at 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.

On five occasions, as alleged in SOR 1.c – 1.g, Applicant brought prohibited electronic devices into secure spaces. After three of those infractions, as alleged in SOR 1.h – 1.j, she did not report her cellphone incidents as required. Although she may have been unclear about the no-cellphone rule before May 2015, it was clear to her thereafter. Nonetheless, she broke that rule at least six more times. To her credit, she self-reported on the first two occasions and was informally counseled about the no-cellphone rule by security staff. However, after the next three incidents, when no one else knew that she had brought her cellphones into the SCIF, and because she feared the consequences that might ensue, Applicant decided to not comply with the requirement to timely self-report her infractions. Her failures to self-report constituted three more violations of security regulations, which along with the underlying cellphone infractions, were investigated collectively as a single security violation for which she was deemed culpable.

As alleged in SOR 1.a and 1.b, she twice failed to properly secure classified information as required. Despite the fact her desk was in a SCIF, that space was not approved for open storage of classified information when the space was unoccupied. To her credit, Applicant self-reported both violations. After the first document-related incident, it appears the company took no disciplinary action. After the second document-related incident, she was issued a letter of reprimand that addressed both of the events alleged in SOR 1.a and 1.b.

All of the foregoing information requires application of the following AG ¶ 34 disqualifying conditions:

(b) collecting or storing protected information in any unauthorized location;

(g) any failure to comply with rules for the protection of classified or sensitive information; and

(h) negligence or lax security practices that persist despite counseling by management.

I also have considered the potential application of the following AG ¶ 35 mitigating conditions:

(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;

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

(c) the security violations were due to improper or inadequate training or unclear instructions; and

(d) the violation was inadvertent, it was promptly reported, there is no evidence of compromise, and it does not suggest a pattern.

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. All of the foregoing undermines any claim that her conduct in this regard "does not cast doubt on the individual's current reliability, trustworthiness, or good judgment." AG ¶ 35(a) does not apply.

Applicant was credible in her assertions that she has a positive attitude towards her security responsibilities. Yet her cellphone infractions recurred several times after being informally counseled in September 2015 and May 2016. Additionally, and despite being counseled after those incidents, she decided to withhold information about her conduct when no one else was aware of it. Her willingness to withhold information about her security infractions appears to have extended to her failure to report the unalleged fact that she brought a cellphone into a SCIF in 2019. While it is commendable that she disclosed that incident as part of this proceeding, it would have been more consistent with her renewed positive approach to security had she reported it to her security staff when it occurred more than three years ago. AG ¶ 35(b) does not apply.

Applicant at various points in her Answer and her testimony cites a lack of efficiency and follow through by her employer in ensuring that she was properly trained in proper security procedures. There is information in the record that suggests her company may not have followed through on recommendations for remedial measures after each infraction or violation. Nonetheless, available 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. In short, it appears she was properly trained in these matters. She also was trained in the requirement to self-report her infractions when they occur, and she did so after two of her four cellphone infractions and both of her document storage infractions. Despite her awareness of the rules about these matters, she affirmatively decided to stay silent about three of her cellphone infractions. 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. On balance, AG ¶ 35(c) does not apply.

The infractions alleged at SOR 1.c – 1.g were inadvertent, and no information was compromised. Indeed, the infraction at SOR 1.a may not have been entirely Applicant's fault given the apparent mishandling by her co-worker that resulted in the document coming into Applicant's possession. Regardless, because she knew the document was classified even if it was not correctly marked, she bears some responsibility for not properly safeguarding it once it was under her control. She timely self-reported the events addressed in SOR 1.a, 1.b, and 1.g. But her decisions to not self-report the cellphone infractions at SOR 1.c, 1.d, 1.e, and 1.f as required constitute deliberate and multiple violations. Those decisions also suggest a pattern, in that she did not report violations in which she was the only one who knew they had occurred. Even though it was not alleged, she again has not reported another possible infraction involving her company cellphone in 2019. While acknowledging she again feared what consequences might come of this information, she also has rationalized her ongoing failure to report that information based on her own assessment that the device was useless and that it would not matter if she reported the incident. That assessment was not hers to make. Her violation of cellphone rules and her failure to report them preclude application of AG ¶ 35(d).

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 AG 35 mitigating conditions. The security concerns raised under this guideline by the Government's information are resolved against the Applicant.

Personal Conduct

The Government's information that established security concerns under Guideline K also supports the cross-allegations of SOR 1.a – 1.j under Guideline E. The security concern about an individual's personal conduct is expressed in relevant part at AG ¶ 15:

> 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 or sensitive information. Of special interest is any failure to cooperate or provide truthful and candid answers during national security investigative or adjudicative processes.

More specifically, I have considered the following AG ¶ 16 disqualifying conditions:

> (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 individual may not properly safeguard classified or sensitive information; and
>
> (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 individual may not properly safeguard classified or sensitive information. This includes, but is not limited to, consideration of:
>
> > (1) untrustworthy or unreliable behavior to include breach of client confidentiality, release of proprietary information, unauthorized release of sensitive corporate or government protected information;
> >
> > (2) any disruptive, violent, or other inappropriate behavior;
> >
> > (3) a pattern of dishonesty or rule violations; and

(4) evidence of significant misuse of Government or other employer's time or resources.

AG ¶¶ 16(c) and 16(d) do not apply because the information about Applicant's security infractions and violations was addressed under Guideline K and is sufficient for an adverse decision. Accordingly, there is no disqualification established under Guideline E, which is resolved for Applicant.

I also have evaluated this record in the context of the whole-person factors listed in AG ¶ 2(d). I note Applicant's record of excellent performance during her career, the positive recommendations by her current and former supervisors, and her wealth of professional accomplishments and qualifications. Additionally, her charitable efforts in the community reflect well on her character. However, this positive information is not sufficient to overcome the security ramifications of her multiple and, at times, deliberate security violations, and the reasonable security concerns raised by the Government's information have not been mitigated. In addition to the need to abide by rules and procedures for safeguarding classified information, a fundamental tenet of the Government's industrial security program involves a willingness by cleared individuals to report or disclose adverse information even at the cost of their own interests. Eligibility for access to classified information imposes a fiduciary obligation that requires individuals to place the national interest in protecting that information ahead of their own interests. Because that did not occur on multiple occasions here, doubts about Applicant's suitability remain. Protection of the interests of national security is the principal focus of these adjudications. Accordingly, those doubts must be resolved against the Applicant's request for clearance.

Formal Findings

Formal findings 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:	AGAINST APPLICANT
Subparagraphs 1.a – 1.j:	Against Applicant
Paragraph 2, Guideline E:	FOR APPLICANT
Subparagraph 2.a:	For Applicant

Conclusion

Based on all of the foregoing, it is not clearly consistent with the interests of national security for Applicant to have access to classified information. Applicant's request for a security clearance is denied.

MATTHEW E. MALONE
Administrative Judge