DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
----------	)	ISCR Case No. 14-02505
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Ray T. Blank, Esquire, Department Counsel
For Applicant: *Pro se*

08/01/2016

_____

Decision

_____

MARSHALL, Jr., Arthur E., Administrative Judge:

Statement of the Case

On November 18, 2014, the Department of Defense (DOD) Consolidated Adjudications Facility (CAF) issued Applicant a Statement of Reasons (SOR) detailing security concerns under Guideline M (Use of Information Technology Systems).[1] In a December 4, 2014, response to the SOR, she admitted the allegations and requested a determination based on the written record. On July 30, 2015, the Government issued a File of Relevant Material (FORM) with seven attachments. Applicant timely responded to the FORM with additional materials. Based on my review of the case file and submissions, I find Applicant mitigated use of information technology security concerns.

Findings of Fact

Applicant is a 56-year-old senior systems engineer who has worked for the same defense contractor since 1980. She married in 1992 and has one teenage child. She has earned a college degree.

[1] The action was taken under Executive Order 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; DOD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the adjudicative guidelines (AG) effective within the DOD on September 1, 2006.

In May 2012, Applicant's employer began an investigation based on a report alleging that Applicant connected her approved portable electronic device (PED) to her restricted personal computer. Applicant knew this was a violation of company security policy. (FORM, Item 6) It also looked into two earlier incidents from 2009 and 2011, respectively. Applicant previously had not been apprised these prior incidents were significant issues of concern. Specifically, it was found that in 2009, she had downloaded software to update her PED from the Internet onto a company computer, an act violating company policy. As well, she was cited for violating computer systems and electronic media policy in 2011 by synching her PED to a company computer.

After the investigation, it was determined that Applicant had performed the three acts at issue, culminating in the following SOR allegations: 1) Applicant violated company procedure [X] (Internet Usage) in January 2009 by downloading software from the Internet for the PED she used at work, which was personally purchased, but required by the corporation, and installing it on a company computer without authorization (SOR allegation 1.b)[2]; 2) Applicant violated company Procedure [Y] (Computer Systems and Electronic Media) by syncing a PED to a company computer in November 2011 (SOR allegation 1.c), and 3) Applicant knowingly violated the company's restricted security policy in May 2012 by connecting her PED into a restricted computer, and by keeping it inside a restricted program facility (SOR allegation 1a). In June 2012, as self-reported by Applicant on her July 2012 security clearance application (SCA), she was disciplined for negligence in mishandling hardware in 2012 and downgraded in security clearance after having her Sensitive Compartmented Information (SCI) access revoked. This occurred despite the finding that there had been no compromise. She was also reassigned and suspended for two weeks without pay. In November 2014, an SOR was issued, citing to the three allegations noted above.

Applicant admitted all SOR allegations. In doing so, she noted that she had not been able to "procure" a copy of corporate procedures in effect before September 2015.[3] Elsewhere, she noted that the version available to employees is dated May 2012.[4] It is unclear whether she was originally given the version or versions in effect in 2009, 2011, and before May 2012. There is no documentary evidence she attended any information technology-based security training, if offered.

In mitigation to the allegations, Applicant offered the following additional facts. Regarding the 2009 incident, Applicant reported that employees were required to

[2] The FORM does not include a copy of company regulations [X] or [Y], which are at issue in allegations 1.b and 1.c.

[3] FORM Response, memo dated Oct. 9, 2015, at 6. *But see* FORM, Item 6, indicating she was given a copy of these procedures in June 2015. Therefore, the evidence is in conflict regarding whether she was ever provided a copy of these earlier editions or whether they were otherwise available to her. There is no copy of these regulations in the FORM.

[4] FORM Response, memo dated Oct. 9, 2015, at 8.

provide their own PED (*e.g.*, Blackberry) for work. Applicant's PED was used so she could have timely and convenient access to her schedule and personnel records, none of which was considered classified. Her PED was specifically approved and sealed by building security for use in restricted areas. The software she obtained to synch with her PED was downloaded onto an unclassified office computer, which was a common practice for employees to update their PEDs and backup data. Applicant noted, "(m)anagement was aware that I had the PED, I had in fact already had it approved and sealed by security to allow for usage in restricted areas, so it seemed logical that security would be aware that software had to be downloaded in order to make the PED functional."[5]

As for the 2011 incident, Applicant admits she synced her company approved PED to an unclassified company computer outside the restricted area, and stresses that the computer was not a restricted computer. She notes that her PED was registered with the company for use in restricted areas and the company had sealed the window through which the PED could be synced to a similar PED. Moreover, her PED was not compatible to synch with a restricted computer as it was not a Bluetooth device, her restricted computer at the time had no working USB portal, and no classified information was on her PED. It was a common practice for employees to synch their PEDs through unclassified computers to make them functional because (a) all data is lost if the battery is not kept charged and (b) the only way to back up the data on a PED is to synch it with a computer because of the PED's limited storage. She was not aware that synching a PED with an unclassified computer violated any policies, noting "I regret that I did not recognize that this common practice throughout [the company] constituted a violation."[6] Given the circumstances and her understanding at the time, she thought it was permissible for her to use the unclassified computer to sync her approved PED. At the time, she was not informed that she had violated any policies.[7]

The 2012 incident involved a new PED Applicant had purchased. It did not come with a charger that could be directly plugged into an electrical wall outlet. It could only be charged via a USB plug. In May 2012, Applicant was late for a meeting and discovered her PED battery was very low. If the battery became depleted, her PED would lose all new information. Applicant did not want to leave her PED openly in a hallway as it charged on one of the available unclassified computers, and there was no available USB plug in the area to which she was headed for her meeting. She purposefully retreated to her office, where she logged off and locked her computer, which had its USB port disabled. She then used that computer's USB port as a conduit for electrically recharging her PED. She had previously been told by the support desk personnel that with these precautions, such charging was permitted. Applicant stresses that her actions were general practices within her unit. After she was interviewed over

[5] FORM Response, memo dated Oct. 9, 2015, at 7.

[6] FORM Response, memo dated Oct. 9, 2015, at 9.

[7] FORM Response, memo dated Oct. 9, 2015, at 9.

the matter in June 2012, she was given a copy of the regulations at issue in SOR allegations 1.b and 1.c.[8]

Since that time, Applicant has been apprised of her violations and of the current rules and regulations. She now understands the regulations and the reasons behind them. She regrets her prior laxity. By all accounts, Applicant is a friendly, hard-working, and personable employee and colleague. Her collegiality helps make for a better work place.[9] A work peer finds her to be "honest, trustworthy, conscientious . . . and capable of conducting work on secure and sensitive material."[10] That peer does not believe the allegations reflect her character or indicate how she will perform with respect to secure materials in the future. Another colleague notes that Applicant is dependable and has learned from her mistakes regarding the office computers and their system.[11]

A final colleague wrote on behalf of Applicant. He has had both a DOD security clearance and SCI clearance since the 1980s. He has worked with and known Applicant for almost 20 years and knows her to be trustworthy.[12] He wrote that:

> during the 2009 – 2011 time period it was common for people working in unclassified environments to have PEDs (blackberries, Palm Pilots, etc.). I did not use one, but they were commonly connected/sync'd with company computers. I know that some of these devices were personal and that some were provided by the company. According to my records, the first Information Security Awareness training I had for unclassified computers was on 01/04/2011. I do not have training records prior to that. It is possible that the training was not clear or did not cover whether personal versions of these items were "approved" to be connected to company computers. I have looked but cannot find copies of the Corporate Policies from that time period. I know personally we had this issue with USB thumb drives/memory sticks. It may have been unclear to [Applicant] what was permitted to be installed or connected to a company machine.[13]

Policies

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

[8] FORM, Item 6.

[9] FORM Response, Attachment 2, reference dated Oct. 2, 2015.

[10] FORM Response, Attachment 3, reference dated Sep. 30, 2015.

[11] FORM Response, Attachment 4, undated reference.

[12] FORM Response, Attachment 5, reference dated Oct. 8, 2015.

[13] FORM Response, Attachment 5, reference dated Oct. 8, 2015.

disqualifying conditions and mitigating conditions, which are used 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 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 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, an "applicant is responsible for presenting witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by applicant or proven by Department Counsel and has the ultimate burden of persuasion to obtain a favorable security decision."

One who seeks access to classified information enters into a fiduciary relationship with the Government based on trust and confidence. This relationship transcends normal duty hours. Decisions include consideration of the possible risk an applicant may deliberately or inadvertently fail to safeguard 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

The use of information technology systems security concern is found at AG ¶ 39:

> Noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about [one's] reliability and trustworthiness, calling into question their willingness or ability to protect sensitive systems, networks, and information.[14]

AG ¶ 40 describes conditions that could raise a security concern and may be disqualifying. The following sections are potentially applicable:

[14] Information Technology Systems include all related computer hardware, software, firmware, and data used for the communication, transmission, processing, manipulation, storage, or protection of information.

a. illegal or unauthorized entry into any information technology system or component thereof;

e. unauthorized use of a government or other information technology system; and

f. introduction, removal, or duplication of hardware, firmware, software, or media to or from any technology system without authorization, when prohibited by rules, procedures, guidelines, or regulations.

Applicant admits the three allegations raised. Consequently, the above disqualifying conditions are applicable.

Conditions that could mitigate the use of information technology systems security concerns are provided under AG ¶ 41. The following is potentially applicable:

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

Applicant's actions can be considered remote since they occurred between 2009 and early May 2012, and were all related to the same tasking. The facts indicate Applicant did not initially receive a copy of the procedures at issue in, at least, the two earliest incidents, nor was she contemporaneously apprised that her acts were considered violations. In none of the violations were secure or classified information compromised. Over four years have passed since Applicant's last misuse.

Since her 2012 reprimand for the three incidents, Applicant has not experienced another security issue concerning information systems security. She has studied her company's current procedures. Members of her company team have vouched for her trustworthiness. They have expressed their satisfaction that Applicant learned from these incidents and will not let such lapses happen again. Applicant provided persuasive evidence to show that sufficient time has passed since the incidents, that any security issues are unlikely to recur, and that her current reliability, trustworthiness, and good judgment are not in doubt. Moreover, I am convinced that Applicant is remorseful for her actions, possesses a positive attitude toward the discharge of her security responsibilities, and will not repeat the behavior. AG ¶ 41(a) applies.[15]

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

[15] While mitigating condition 41(b) could apply to the earlier incidents, the evidence does not support a finding that Applicant's conduct was the result of having "no other timely alternative readily available."

adjudicative process factors listed at AG ¶ 2(a). Under AG ¶ 2(c) sets forth the need to utilize a whole-person evaluation.

I considered the potentially disqualifying and mitigating conditions in light of all the facts and circumstances surrounding this case. I incorporated my comments under the guideline at issue in my whole-person analysis. Applicant is a 56-year-old naturalized United States citizen who has worked for the same defense contractor since 1980. She now serves as a senior systems engineer. She married in 1992, has one child, and has earned a college degree. She is highly regarded by her employer and work peers for her congeniality, hard work, diligence, and work performance.

I also considered that Applicant's last security incident occurred in early 2012 without recurrence. Moreover, I considered the lack of training it appears she was offered before that time and the mission requirements of her position. Moreover, I have also noted the apparent conflict between her company's written policies, everyday employee practice, and the input of the technical specialists. Finally, I also took into account the fact that Applicant fully admitted her mistakes and has taken initiative in seeking improvement. Her ability to follow the procedures now in place seems apparent from both her own comments and her multiple, positive recommendations. All of this demonstrates permanent behavioral changes toward security issues and the unlikeliest chance of recurrence. Applicant met her burden with sufficient evidence to mitigate the security concerns arising under Guideline M.

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 M:	FOR APPLICANT
Subparagraphs 1.a-1.c:	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 grant Applicant a security clearance. Eligibility for access to classified information is granted.

_____
Arthur E. Marshall, Jr.
Administrative Judge