DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 11-11062
	)	
Applicant for Security Clearance	)	

Appearances

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

04/30/2013

Decision

O'BRIEN, Rita C., Administrative Judge:

Based on a review of the pleadings, the Government's File of Relevant Material (FORM), and the exhibits, I conclude that Applicant has not mitigated the security concerns raised under Guidelines K (Handling Protected Information), M (Use of Information Technology Systems), and E (Personal Conduct). Her request for a security clearance is denied.

Statement of the Case

On November 29, 2012, the Department of Defense (DOD) issued a Statement of Reasons (SOR), under Executive Order 10865, *Safeguarding Classified Information Within Industry,* dated February 20, 1960, as amended; Department of Defense (DOD) Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program (Directive),* dated January 2, 1992, as amended; and the adjudicative guidelines (AG) implemented by the DOD on September 1, 2006. The SOR listed security concerns addressed in the Directive under Guidelines K, M, and E. In her December 21, 2012, Answer to the SOR, Applicant admitted all six allegations. She also requested a decision without a hearing.

Department Counsel for the Defense Office of Hearings and Appeals (DOHA) prepared a written presentation of the Government's case in a FORM dated March 20,

2013. The FORM was forwarded to Applicant, along with seven evidentiary documents (Items 1 through 7). Applicant received the FORM but did not submit a response. The case was assigned to me on April 26, 2013, for an administrative decision based on the record.

Procedural Matters

I take administrative notice of the following requirements set out at §§ 1-200 and 5-308 of the *National Industrial Security Program Operating Manual* (*NISPOM*), DOD 5220.22-M, dated February 28, 2006, and provided in Department Counsel's FORM. (Item I):

> **§1-200. General.** Contractors shall protect all classified information to which they have access or custody. A contractor performing work within the confines of a Federal installation shall safeguard classified information according to the procedures of the host installation or agency.
>
> §**5-308. Protection of Combinations to Security Containers, Cabinets, Vaults and Closed Areas.** Only a minimum number of authorized persons shall have knowledge of combinations to authorized storage containers. Containers shall bear no external markings indicating the level of classified material authorized for storage.
>
> > a. A record of the names of persons having knowledge of the combination shall be maintained.
> >
> > b. Security containers, vaults, cabinets, and other authorized storage containers shall be kept locked when not under the direct supervision of an authorized person entrusted with the contents.
> >
> > c. The combination shall be safeguarded in accordance with the highest classification of the material authorized for storage in the container.
> >
> > d. If a record is made of a combination, the record shall be marked with the highest classification of material authorized for storage in the container.

Findings of Fact

Applicant's admissions in response to the SOR are incorporated as findings of fact. After a thorough review of the pleadings and evidence, I make the following additional findings.

Applicant is a 49-year-old high school graduate. As of the date of her June 2011 security clearance application, she had been married since 2005, and had three children and three step-children between the ages of 23 and 29. She has held a secret security clearance since 2002. She has worked for her current employer, a defense contractor, since 1985.[1] Her position is senior configuration analyst. (Items 4, 5)

Between about December 2008 and December 2010, Applicant saved passwords for classified computer systems and combinations for classified container locks in a spreadsheet on her unclassified work computer. She had numerous passwords, and saved them in an Excel spreadsheet for ease of recall. She considered her work computer to be "secure"[2] and did not realize that saving the information on what she considered a "secure" computer was a security violation. By December 2010, she stopped saving new passwords and combinations to her spreadsheet because she had fewer new passwords and combinations to remember. She continued to use the Excel workbook that contained the spreadsheet. However, after December 2010, she no longer used the specific spreadsheet with the previously used passwords and combinations. (Items 5, 6, 7)

In about February 2011, Applicant was compiling an instruction memorandum using the Excel workbook. She was also having trouble accessing her company's computer system from her home. She decided to send the workbook to her home computer using her personal email account, so that she could use it while working from home. She needed it to complete the instruction memorandum and to use the contact information it contained. During her 2011 security interview, she stated that she had not been using the spreadsheet containing the passwords and combinations, so she forgot that the workbook included the spreadsheet. Between February and March 2011, Applicant emailed the workbook with the combinations to classified containers to her unclassified home computer about three times. (Item 5, 7)

The general requirement at NISPOM §1-200 states that contractors must protect classified information to which they access or custody. Specifically, §5-308 requires that "combinations be protected in accordance with the highest classification of the material authorized for storage in the container." Records of the lock combinations must be marked with the highest classification of material stored in the container. The file contains no information on the classification level of the material stored in the containers. The file also does not indicate the classification level of the computer systems for which Applicant stored passwords. (Item II)

[1] Applicant entered 2004 as her start date with her current employer because she thought she was required to enter employment only during the previous seven years. She provided the correct information at her security interview. (Item 5)

[2] Other than the word "secure," the file does not explain Applicant's understanding of the status of her work computer. As this decision is based on the written record, Applicant cannot be questioned to determine if by "secure," Applicant meant that she thought her computer was approved to store classified information. (Item 5)

On March 19, 2011, Applicant's security office contacted her about sending classified information to her personal email account. She was informed it was a serious violation and that her security clearance was being suspended. In May 2011, her security officer entered an incident report in the DOD security database, stating,

> [Applicant] has been found culpable for an intentional security violation. [Applicant] knowingly had combinations and a password to classified containters (*sic*) and a classified information system saved in an Excel spreadsheet on her unclassified computer. She further compromised the information by sending it to her personal [---] email account. The range of disipline (*sic*) is suspension without pay with a written reprimand to termination, depending on the level of compromise and employee intent. (Item 7)

In June 2011, Applicant was officially reprimanded, received a written warning, and was suspended without pay for one week for violation of a security rule. She was transferred to other duties that did not require a security clearance, and she was required to attend security training. She completed the training in July 2011. Before July 2011, Applicant had received annual security training. (Items 5, 7)

During her August 2011 security interview, Applicant stated she knew she was not permitted to send technical information to a personal email account, but did not believe the workbook was a security issue because it contained only contact information and instructions regarding work tasks. She did not remember the workbook also included the spreadsheet of passwords (although some were apparently no longer in use at the time) and combinations to classified containers. She now understands that saving passwords to classified systems and combinations to classified containers, and sending such information to a personal email account, are security violations. She had no security violations or job performance issues before this event. She has no intention to engage in such conduct in the future. (Items 5, 6)

On October 3, 2012, Applicant signed an interrogatory stating that she has complied with security regulations and employee rules since this event. She memorizes passwords, does not write them down, and does not use patterns. She has not emailed work-related information to her personal email account. The incident has been discussed in team, section, and department meetings. (Item 6)

Policies

Each security clearance decision must be a fair and commonsense determination based on examination of all available relevant and material information, and consideration of the pertinent criteria and adjudication policy in the AG.[3] Decisions must also reflect consideration of the factors listed in ¶ 2(a) of the Guidelines, commonly referred to as the "whole-person" concept. The presence or absence of a disqualifying

[3] Directive. 6.3.

or mitigating condition does not determine a conclusion for or against an applicant. However, specific applicable guidelines are followed whenever a case can be measured against them as they represent policy guidance governing the grant or denial of access to classified information. In this case, the pleadings and the information presented by the parties require consideration of the security concerns and adjudicative factors addressed under Guidelines K, M, and E.

A security clearance decision is intended only to resolve the question of whether it is clearly consistent with the national interest[4] for an applicant to either receive or continue to have access to classified information. 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.[5] A person who has access to classified information enters into a fiduciary relationship with the Government based on trust and confidence. Therefore, 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 her or his 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.[6]

Analysis

Guideline M, Use of Information Technology Systems

AG ¶ 39 expresses the security concern related to use of information technology systems:

> Noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual's reliability and trustworthiness, calling into question the willingness or ability to properly protect sensitive systems, networks, and information. Information Technology Systems include all related computer hardware, software, firmware, and data used for the communication, transmission, processing, manipulation, storage, or protection of information.

---

[4] *See Department of the Navy v. Egan*, 484 U.S. 518 (1988).

[5] *See Egan,* 484 U.S. at 528, 531.

[6] *See Egan;* AG ¶ 2(b).

AG ¶ 40 describes disqualifying conditions that could raise a security concern, including the following relevant conditions:

> (d) downloading, storing, or transmitting classified information on or to any unauthorized software, hardware, or information technology system;

From 2008 to 2010, Applicant engaged in unauthorized use of an information technology system when she stored passwords for classified computer systems and lock combinations for classified containers on her unclassified company computer. She also transmitted this classified information to her unclassified home computer. Disqualifying condition AG ¶ 40(d) applies.

AG ¶ 41 provides the following relevant mitigating conditions:

> (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; and
>
> (c) the conduct was unintentional or inadvertent and was followed by a prompt, good-faith effort to correct the situation and by notification of a supervisor.

Applicant states that she did not engage in these actions intentionally. However, she has worked for the same employer for many years, and received security training every year. Given her annual security training, it is unlikely that during the two years when Applicant created and maintained these lists, she did not realize that passwords for classified files and combinations to classified safes constituted data that must be protected. Her belief that her work computer was "secure" and so could be used for this data, is not convincing. Even if true, that rationale does not apply to her home computer. She knew her home computer was unclassified, yet she forwarded the workbook containing classified information to her home three separate times. There is no record evidence that she contacted security officers to determine if it was appropriate to transmit the information, or to alert them that she had done it. Her conduct was not revealed until the security department discovered it. Applicant's actions are not recent; however, they occurred in the normal course of her employment, not in unusual circumstances. Her conduct casts doubt on her reliability and good judgment. AG ¶¶ 41 (a) applies in part, and AG ¶ 41(c) does not apply.

Guideline K, Handling Protected Information

AG ¶ 33 expresses the security concern pertaining to handling protected information:

> Deliberate or negligent failure to comply with rules and regulations for protecting classified or other sensitive information raises doubt about an

> individual's trustworthiness, judgment, reliability, or willingness and ability to safeguard such information, and is a serious security concern.

The following disqualifying conditions under AG ¶ 34 raise a security concern:

> (b) collecting or storing classified or other protected information at home or in any other unauthorized location;
>
> (c) loading, drafting, editing, modifying, storing, transmitting, or otherwise handling classified reports, data, or other information on any unapproved equipment **i**ncluding but not limited to any typewriter, word processor, or computer hardware, software, drive, system, gameboard, handheld, "palm" or pocket device or other adjunct equipment; and
>
> (g) any failure to comply with rules for the protection of classified or other sensitive information.

Applicant's storage of passwords to classified systems and the combinations to classified safes on an unclassified computer violated NISPOM §§ 1-200. In addition, according to NISPOM 5-308(c) and §5-308(d), the combinations to classified containers that Applicant compiled between 2008 and 2010 would be classified at the highest level of the information stored in the containers. As classified information, the combination list was required to be stored only in classified computers. However, Applicant stored the list on her unclassified work computer. In February and March 2011, she transmitted it three times via her unclassified home email account to her unclassified home computer. AG ¶¶ 34(b), (c), and (g) apply.

AG ¶ 35 provides conditions that could mitigate security concerns, including the following relevant 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; and,
>
> (c) the security violations were due to improper or inadequate training.

Applicant stored classified information on her unclassified work computer between 2008 and 2010, three to five years ago. She emailed the information to her home unclassified computer two years ago. Her conduct is not recent. Although the file does not contain extensive information on Applicant's conduct since the event, it appears that she has received additional security training, and no further security

violations have occurred. Her conduct is not frequent. However, given her years of security training, Applicant's conduct raises questions about her reliability and judgment. AG ¶ 35(a) applies in part and AG ¶ 35(b) applies. Applicant received annual security training over many years; AG ¶ 35(c) does not apply.

Guideline E, Personal Conduct

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

> Conduct involving questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations can raise questions about an individual's reliability, trustworthiness and ability to protect classified information. Of special interest is any failure to provide truthful and candid answers during the security clearance process or any other failure to cooperate with the security clearance process.

AG ¶ 16 describes conditions that could raise a security concern and may be disqualifying. The following conditions are relevant:

> (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 person may not properly safeguard protected information.

For two years, Applicant maintained classified information on her unclassified work computer. She then sent that information to her home computer, which she knew to be unclassified. Her conduct demonstrated questionable judgment, unreliability, and a lack of awareness of her responsibilities toward classified information. AG ¶ 16(c) applies.

AG ¶ 17 provides conditions that could mitigate security concerns under personal conduct guideline. The following conditions are relevant:

> (c) the offense is so minor, or so much time has passed, or the behavior is so infrequent, or it happened under such unique circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment; and
>
> (d) the individual has acknowledged the behavior and obtained counseling to change the behavior or taken other positive steps to alleviate the stressors, circumstances, or factors that caused untrustworthy, unreliable, or other inappropriate behavior, and such behavior is unlikely to recur.

The offense Applicant committed is not minor: security violations undermine the industrial security program that protects classified information. Applicant's conduct casts doubt on her reliability. Regarding mitigating condition AG ¶ 17(d), Applicant has received additional security training, and states that she now understands the security rules, she has taken "this very hard," and has learned from her errors. However, I balance these facts against the fact that Applicant engaged in this behavior over a period of three years, from 2008 to 2011. I cannot find that the situation is unlikely to recur, given that Applicant engaged in this behavior over an extensive period, during a time when she was receiving security training. AG ¶¶ 17 (c) and (d) do not apply.

Whole-Person Concept

Under the whole-person concept, an administrative judge must evaluate the applicant's security eligibility by considering the totality of the applicant's conduct and circumstances. I have evaluated the facts and applied the appropriate adjudicative factors. I have reviewed the record in the context of the following whole-person factors:

> 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.

Without an in-person hearing, or further evidence of Applicant's performance and character through performance evaluations and references, I cannot fully assess her credibility and character. However, it appears from the record that she has positive attributes including her work for a defense contractor for the past 28 years.

However, Applicant engaged in serious security violations when she stored classified information on her unclassified work computer. She also transmitted that classified information via her unclassified email account three times, and then stored it on her unclassified home computer**.** Each time she left classified information on an unclassified computer—at work and at home—she placed that classified information at risk of disclosure. It is unlikely that Applicant was unaware of the prohibition against such actions--given her annual security training--or that she could have remained unaware of it for three years. The security personnel who were most familiar with the circumstances surrounding the events determined that she should receive a reprimand, have her security clearance suspended, be suspended from work for one week without pay, and be transferred to unclassified duties.

The awarding of a security clearance is not a once in a lifetime event, but is based on applying the disqualifying and mitigating conditions to the evidence presented. Under Applicant's current circumstances, a clearance is not warranted. Should she be

afforded an opportunity to reapply for a security clearance in the future, having established changed circumstances, she may be able to demonstrate evidence of security worthiness. However, the record evidence at this time fails to satisfy the doubts raised about Applicant's suitability for a security clearance. For all these reasons, I conclude Applicant has not mitigated the security concerns raised by the cited adjudicative guidelines.

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 as follows:

Paragraph 1, Guideline E:	AGAINST Applicant
Subparagraphs 1.a – 1.b	Against Applicant
Paragraph 2, Guideline K:	AGAINST Applicant
Subparagraphs 1.a – 1.b	Against Applicant
Paragraph 3, Guideline M:	AGAINST Applicant
Subparagraphs 1.a – 1.b	Against Applicant

Conclusion

In light of the foregoing, it is not clearly consistent with the national interest to grant Applicant access to classified information. Applicant's request for a security clearance is denied.

RITA C. O'BRIEN
Administrative Judge