DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 10-07070
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Fahryn Hoffman, Esquire, Department Counsel
For Applicant: *Pro se*

December 12, 2011

Decision

HENRY, Mary E., Administrative Judge:

Based upon a review of the pleadings, exhibits, and testimony, Applicant's eligibility for access to classified information is granted.

Statement of the Case

Applicant signed an Electronic Questionnaire for Investigations Processing (e-QIP) on August 7, 2007. The Defense Office of Hearings and Appeals (DOHA) issued Applicant a Statement of Reasons (SOR) on April 8, 2011, detailing security concerns under Guideline K, handling protected information, and Guideline E, personal conduct, that provided the basis for its preliminary decision to deny her a security clearance. The action was taken under Executive Order 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the *Adjudicative Guidelines For Determining Eligibility for Access to Classified Information* (AG) implemented on September 1, 2006.

Applicant received the SOR on April 19, 2011. She answered it on May 3, 2011 and requested a hearing before an administrative judge. DOHA received the request, and Department Counsel was prepared to proceed on June 2, 2011. I received the case assignment on June 20, 2011. DOHA issued a Notice of Hearing on July 6, 2011, and I convened the hearing as scheduled on July 26, 2011. The Government offered exhibits marked as GE 1 through GE 5, which were received and admitted into evidence without objection. Applicant testified. She submitted AE A through AE J, which were received and admitted into evidence without objection. DOHA received the hearing transcript (Tr.) on August 3, 2011. I held the record open until August 9, 2011, for Applicant to submit additional matters. Applicant timely submitted AE K through AE DD, which were received and admitted without objection. The record closed on August 9, 2011.

Findings of Fact

In her Answer to the SOR, Applicant admitted the factual allegations in ¶¶ 1.a, 1.b, 2.a, and 2.d-2.g of the SOR. Her admissions are incorporated herein as findings of fact. She denied the factual allegations in ¶¶ 2.b and 2.c of the SOR.[1] She also provided additional information to support her request for eligibility for a security clearance. After a complete and thorough review of the evidence of record, I make the following additional findings of fact.

Applicant, who is 58 years old, works as a photo technician for a Department of Defense contractor. She has worked in her job and location for 18 years, although her employer changed in 2009. She has received numerous performance awards as a civilian employee, including a team excellence award in September 2009 for her exceptional contribution to an airdrop test and a team excellence award in November 2010 for her work over a two-month period on photographing two vehicles both day and night.[2]

She served in the United States Marine Corps from 1972 to 1974 and from January 1979 until November 1990. She received an honorable discharge from the Marine Corps. During her nearly 14 years of military service, she held a security clearance without any violations. While in the Marine Corps, she received a National Defense Service Medal, three good conduct medals, a meritorious mast, and numerous letters of appreciation. As a Marine, she worked as a postal clerk for three years. The

[1]When SOR allegations are controverted, the Government bears the burden of producing evidence sufficient to prove controverted allegations. Directive, ¶ E3.1.14. "That burden has two components. First, the Government must establish by substantial evidence that the facts and events alleged in the SOR indeed took place. Second, the Government must establish a nexus between the existence of the established facts and events and a legitimate security concern." *See* ISCR Case No. 07-18525 at 4 (App. Bd. Feb. 18, 2009), (J. Billett, concurring and dissenting, in part) (citations omitted). The guidelines presume a nexus or rational connection between proven conduct under any of the criteria listed therein and an applicant's security suitability. *See* ISCR Case No. 08-06605 at 3 (App. Bd. Feb. 4, 2010); ISCR Case No. 08-07290 at 2 (App. Bd. Nov. 17, 2009).

[2]GE 1; AE G; Tr. 119-120.

Marine Corps then trained her as a photographer, a duty she performed for the remaining years of her military service.[3]

Applicant married in 1974 and again in 1993. She has been divorced since 2004. She has a daughter, who is 36 years old, and a son, who is 32 years old. Her 88-year-old mother lives with her, as does her daughter and 4-year-old granddaughter. She attended college, but did not receive a degree.[4]

The SOR raises the following security violations in paragraph 1:

> a. In April 2010, you failed to properly secure a classified security card, in violation of paragraphs 5-100, 5-303 of the National Industrial Security Program Operating Manual (NISPOM), February 2006.
>
> b. In April 2009, you failed to properly secure a classified security card, by taking the classified card home instead of replacing it in a secure container, in violation of paragraphs 5-100, 5-303 of the NISPOM, February 2006.

The SOR raises the following personal conduct issues in paragraph 2:

> a. You received two written reprimands from your employer for security violations, as set forth in paragraph 1, above.
>
> b. In May 2010, you received an oral reprimand for violating work rules and dishonesty by overcharging time on your time card in January 2010.
>
> c. In May 2010, you received an oral warning for violating work rules by discussing the security violation set forth in subparagraph 1.a., above.
>
> d. In May 2009, you received a written warning for a security violation for failing to use seatbelts in a vehicle on the Armed Forces installation.
>
> e. In February 2006, you received a written warning and placed on 6 months of probation for improperly securing an individual's Social Security Number and other personal information. This was your second such warning.
>
> f. In August 2005, you received an oral warning for violating procedures.
>
> g. In May 2010, as a result of the security and rules violations set forth in subparagraphs 2.a. through 2.f., your employer filed a Last Chance

[3]GE 1; AE E; AE F; AE H; AE J; Tr. 41.

[4]GE 1; Tr. 40-42.

Agreement whereby any further violation could result in employment termination.

In 2005, the Department of the Army began implementing changes in the rules and procedures on how promotional photographs were to be digitally photographed and sent to D.[5] Problems with the computer programs occurred, including problems with the background color, with the account number and code, font size, location of data, and the computer software. During the months of implementation of the new processes, Applicant and her co-workers kept in constant contact with D to resolve the problems encountered. On August 15, 2005, management assigned Applicant to the studio work area where she worked when needed, which was not every day. She prepared three photographs and submitted them to her government counterpart, who returned any photographs with a problem to be corrected. Her photo submissions had the wrong format for the date and one photo was the wrong size. Two of the three photographs were returned to Applicant for correction. She corrected the size on the one photograph, but her date corrections remained wrong. She met with management the day after this incident and advised them that the problem would continue as there were no standard operating procedures. Within 24 hours, management suggested to her lead, not her, that a template for photograph captions be prepared to eliminate issues with incorrect formats. Applicant denies receiving an oral warning for the errors on this day. However, the record indicates that an oral warning was given on this day for not following proper procedures when entering information onto the photo system, not paying attention to processing data and following prescribed procedures, and not filling out the photo log book correctly. Applicant signed this document on August 29, 2005. No sensitive information was compromised as a result of this incident.[6]

Six months later, in February 2006, Applicant again worked in the studio area, taking photographs. Once she completed the photograph, her duties required her to insert a name, date, rank, and social security number on the photograph. During the course of the day, she took several photographs, inserted the information, and placed the completed photograph in the desk because this small office did not have a safe or other locked area to place or store cameras, cards, or data. After working in the office for several hours, Applicant had an opportunity to go to the ladies room. She left a photograph and related information in a folder on the desk under the computer keyboard and closed the door to the room, asking a co-worker to make sure no one entered the room. When she returned five minutes later, she discovered the folder and information gone because a Mr. R had entered the room through another door, and after searching, Mr. R. discovered the folder with the information. After this incident, management placed a safe in the room to store cameras, cards, and data. Applicant denies receiving an oral or written statement because of this incident. The record contains an employee discipline report dated February 9, 2006, which shows a written warning and six months of probation for Applicant. The report is signed only in the

[5]The full name for D will not be used in this decision.

[6]Response to SOR; GE 3, p. 7; Tr. 80-82.

employee box, but the signature is not legible. Her managers did not sign this document; thus, this document does not constitute a valid disciplinary report.[7]

In April 2009, one week after being assigned to a new section, Applicant reported to work at 3:00 a.m. for the purpose of asking her supervisor for a return to the day shift. She was not accustomed to working nights and had begun to experience problems with sleeping and staying awake. On the night in question, management assigned her to a two-part program to take photographs. One program part involved classified photographs, and the second program part involved unclassified photographs. Applicant signed out a blank classified card on which photographs were to be taken, located a required blue bag for the card, as she had not yet been assigned a blue bag, placed the card into the blue bag, locked the blue bag, placed the blue bag into a larger blue bag, locked the second blue bag, and placed the blue bag into her briefcase. She assembled her camera equipment and obtained a blank unclassified card for photographs. She drove to the work site. After she arrived, she removed the classified card and inserted it into her camera. She placed the unclassified card in her pocket. At the photograph site, she was told she only needed to take unclassified photographs. She removed the classified card from her camera without taking any photographs and placed it in her purse. She inserted the unclassified card in her camera and took the required photographs. At the end of a 13-hour work day, she returned to her office, removed the unclassified card from her camera, and placed it in the process bin. She worked on paperwork related to her photographs taken that day, then left for home around 7:00 p.m., more than six hours after the end of her usual 10-hour work day. While asleep that evening, she received a telephone call asking about a classified card. Initially, she denied having a classified card, but then remembered that she had signed out a classified card. She checked her bag, found the blank classified card, and called her office with this information. She dressed and returned to her office before 5:00 a.m with the card. At all times, the blank classified card remained within her positive control and no classified information was compromised.[8]

The next day Applicant's supervisor, Mr. D., removed her from the program. He also advised her that he had spoken to their government counterpart, who told him that as long as there was no data on the card, there was no compromise of national security. Her supervisor also advised her that as long as she had positive control over the card, which she did, the government would not issue a report if the card was returned timely. Her employer's administrative security clerk prepared an incident report. Applicant's supervisor gave her an oral warning at the time. She did not receive any other discipline for this incident in April 2009. Nearly 13 months later, on May 4, 2010, a supervisor, whose identity is not in the file, prepared a discipline report, showing a written warning for this incident. It also indicated that a failure to immediately improve could result in time off or immediate termination. Applicant never saw the discipline report until she opened a package of materials from DOHA related to her hearing. She never signed

[7]Response to SOR; GE 3, p. 6; Tr. 82-84.

[8]Response to SOR; GE 2; GE 3; Tr. 50-56.

this discipline report. On its face, the report states that her signature would indicate she received it. [9]

In early 2009, Applicant received a telephone call from her daughter, advising that Applicant's elderly mother had passed out, had fallen and hit her head, and was being taken to the hospital. Applicant panicked. She left the office and entered her personal vehicle. She drove out of her work grounds without securing her seat belt, a safety violation. The gate guard noticed and gave her a ticket on February 24, 2009. Management prepared an employee discipline report, dated March 31, 2009, for a safety violation, which was her first warning for a safety violation. The report indicated that it was a written warning, and that Applicant did not have any previous warnings.[10] Under the Improvement Required section of the discipline report, she was given 365 days to obey all base traffic laws and speed limits, which she has done. Applicant signed for this disciplinary report.[11]

In late January 2010, substantial rain fell where Applicant lives and works. Significant flooding occurred at her work base, and the Government closed the work base and sent employees home from work. Applicant arrived at work on January 21, 2010. On this date, she worked 5.5 hours before the base was closed. She recorded her time worked and an additional 4.5 hours for weather issues on her approved time sheet. She returned to work on January 22, 2010 as instructed by her team engineer at the photo site. Mr. D, her supervisor, arrived soon after her. He questioned her presence in the office, and she told him about her instructions the previous day. She asked for instructions on how to charge her time, but did not receive clear instructions from Mr. D. Her approved time sheet reflects that she charged five hours for her time on January 22, 2010, after being advised that the Government would pay for her time.[12]

Applicant denies Mr. D formally counseled her in January 2010. The record contains a memorandum for record which Mr. D prepared on January 25, 2010. He indicates that Applicant improperly charged her time on January 22, 2010 and that he counseled her about how to properly charge her time. Her approved employee time sheet, dated January 26, 2010, shows 5 work hours for January 22, 2010. On May 4, 2010, three-and-one-half months later, Mr. D submitted an employee discipline report indicating that Applicant reported improper time on January 21, 2010 and January 22, 2010. He indicated that the disciplinary action was an oral warning for violation of work rules and dishonesty, but he did not list a specific time for improvement. Applicant denies any knowledge of this disciplinary report until she received a package from

[9]Response to SOR; GE 3; Tr. 56.

[10]GE 3 contains a copy of a parking ticket given to Applicant on March 9, 2009 for incorrectly parking her personal car on base. This ticket is not listed in the SOR nor did Applicant receive a written warning for the ticket.

[11]Response to SOR; GE 3; Tr. 79.

[12]Response to SOR; AE BB; Tr. 67-71.

DOHA. Her denial is supported by the fact that her signature is not on the May 4, 2010 disciplinary report. On its face, the report states that her signature would indicate she received it.[13]

Applicant submitted a letter from a Human Resources (HR) deputy, dated July 21, 2011.[14] The HR deputy advised that the employees were not directed to the proper account for time reporting for the emergency situation. The HR deputy further advised that Applicant and the majority of the company's employees were not properly advised on how to charge the flood time. The employees were verbally warned to allow them to correct their time card, not as a disciplinary action. On July 22, 2011, the HR deputy wrote a second letter to explain the purpose of the oral warning documented in Applicant's personnel file. The oral discipline reports were meant to serve as a memorandum for the record only and are not considered a written disciplinary report.[15]

In April 2010, a second security incident occurred. Applicant arrived at work at 4:00 a.m., as she needed to be at a specific work site at 5:30 a.m. Her original assignment had been moved back a few days. Mr. D then told her that he needed her to go to another work site immediately. Mr. D. could not tell her if the job was for classified or unclassified photographs. After she retrieved her cameras and gear, she signed out a blank classified card and a blank unclassified card under the procedures for use at the site. As required, she placed the blank classified card in the blue bag and locked it, then placed the blue bag in her briefcase, which she locked. She placed her briefcase in the government vehicle she was driving. She called for clearance to her destination and drove there. When she arrived, she asked the road guard for permission to enter the work area. The road guard called someone to verify that Applicant had access. After several minutes, the road guard advised Applicant that the photographic shoot had been cancelled. During her wait, Applicant had inserted the blank classified card into her camera. She removed it when she learned she would not be needed at the work site and secured the card in its blue bag and placed it in her brief case, which she locked and placed on the floor of her government vehicle. She drove to her work building, parked her car in the designated, secure government parking area, and walked into the building, leaving her brief case in the locked car.[16]

Mr. D advised that he did not have a project for her around 6:45 a.m. Since Mr. D did not have an immediate assignment for her, she requested and received authorization to take the morning CORE classes. She attended class from 7:30 a.m until noon. During this time, the blank classified card remained locked in the blue bag in her

---

[13]Response to SOR; GE 3; Tr. 67-71.

[14]This letter references severe flooding in early May 2010. Since the letter references an oral warning disciplinary report dated May 3, 2010 for flooding in late January 2010, I find that the letter refers to the January flooding.

[15]AE A; AE B.

[16]Response to SOR; GE 3; Tr. 57-58.

locked brief case in her locked government vehicle. She was the only person who knew where the card was located. She returned to her government vehicle and removed keys to the security bag from her person, unlocked her brief case, and placed the keys in the brief case, which she then closed and turned the combination lock. She believed that the brief case was locked. She drove to her work building and received a new assignment. She never started any new assignment as her work assignments continued to change during the course of the afternoon. She remained in and around her work building, and her government car remained locked and parked in the designed secure government parking area. She kept the card in her car as she had anticipated another photo assignment before the end of her work day. She left work at 5:00 p.m. without returning the blank classified card to its secured box. Applicant acknowledged that she failed to follow procedures for returning the classified blank card and her own procedures for protecting the blank classified cards when she did not return the blank classified card to its secured box. Applicant never took any pictures with the classified card. At all times in question, the card was blank and no classified information was compromised.[17]

After the second incident, Applicant's employer suspended her from work for 14 days. When she returned to work, she met with managers. During this counseling session, management asked if all her questions regarding her recent security incident had been answered. Management also advised her not to disclose any facts about her security incident beyond this meeting. They advised her that she would be transferred to another work area, where she does little work with classified materials, but continues to use her photographic skills. After the meeting, management prepared a disciplinary report for an oral warning. The facts section states as follows:

> [Applicant] was counseled to make certain that all of her questions regarding her recent security incident, for which she was disciplined, have been answered. The . . . Manager, in a meeting with [Applicant] and J. M. on 3 May 10 in J's office, was told that the events and circumstances surrounding her recent infraction are not to be disclosed beyond the confines of J's office, other than to senior [company] management. Furthermore, [Applicant] was told by the group manager that no one else, other that [company] management, needs to know about her situation.

In the Improvement Required section, the report states, "Employee must not complain about or disclose any information regarding her incident involving a security incident." Finally, the Failure to Improve section states, "If [Applicant] discloses or complains about her situation regarding the security incident and subsequent disciplinary action to other employee(s), she may receive a written warning, time off without pay or termination of employment." Applicant's signature is not on this disciplinary report. Applicant denies telling anyone about this incident and her resulting discipline. The

[17] *Id*.

record does not show she has been disciplined for telling co-workers about the security incident in April 2010 as alleged in the SOR.[18]

On May 25, 2010, Applicant again met with management at her company. They required her to sign a broad Last Chance Agreement with no end date. Under the terms of this agreement, if she fails to follow security-related rules or policies, she will be immediately terminated.[19]

The record contains an excerpt from the National Industrial Security Program Operating Manual (NISPOM), DoD 5220.22-M, dated February 28, 2006. In the first paragraph, the NISPOM states:

> Contractors shall be responsible for safeguarding classified information in their custody or under their control. Individuals are responsible for safeguarding classified information entrusted to them. The extent of protection afforded classified information shall be sufficient to reasonably foreclose the possibility of its loss or compromise. *See* Section 5-100. General.
>
> Section 5-303 directs that SECRET material shall be stored in a GSA-approved security container, an approved, vault, or closed area. . .[20]

Requirements for the physical protection of classified material are set out in Section 5-300, *et seq.* The record also contains a copy of the company standard operating procedures (SOP) for use of classified media in 2010. The contractor's SOP 16-001 in paragraph 7 describes the process for signing out, using, storing, and signing in media used for classified images. However, the SOP does not define the term "classified media" or indicate when unclassified media becomes classified media. SOP 16-001, paragraph 7b(1) states, "Keep *positive* control of all classified media *at all times*." SOP 16-001, paragraph 7c(3) requires classified media to be signed in (and properly stored) at the conclusion of the mission. There is no document showing if she had reviewed this SOP. Applicant reviewed the SOP for information system security - classified and for safeguarding classified material in an emergency on July 21, 2011, and for classified media handling for IT systems on April 13, 2011.[21]

Applicant submitted copies of her training certificates for protection of classified information. The documents reflect that she completed numerous training classes for information assurance awareness and for awareness training. She also completed a

---

[18]GE 3. Applicant testified to telling co-workers to "dot their i's and t's" and denies telling anyone about her security violation issue. Tr. 72-77.

[19]GE 3.

[20]The remaining provisions of this section describe the criteria for an approved storage container or area.

[21]GE 4; GE 5; AE X - AE Z.

class on portable electronic devices and removable storage media on March 25, 2009 and April 14, 2009.[22]

Applicant provided 12 recent letters of recommendation and three older letters of recommendation. The majority of these letters are from co-workers and test officers at her place of work. All describe her as trustworthy and reliable. She has excellent work skills and work ethics. They give her high recommendations as an individual and as a worker. None of these individuals indicated any knowledge about the issues raised in the SOR. She could not provide this information to them based on the May 3, 2010 meeting.[23]

In her current position, Applicant seldom works with classified information. When she does work with classified information, she and another employee work together. In the past, Applicant was granted a special White House clearance when the President visited her work area. Department Counsel acknowledged Applicant's forthright testimony at the hearing. She testified credibly at the hearing and always accepted responsibility for her conduct.[24]

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 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, past and present, favorable and unfavorable, in making a decision.

The protection of the national security is the paramount consideration. AG ¶ 2(b) requires that "[a]ny doubt concerning personnel being considered for access to classified information will be resolved in favor of national security." In reaching this decision, I have drawn only those conclusions that are reasonable, logical, and based on the evidence contained in the record.

---

[22]AE D.

[23]GE 3; AE I; AE K; AE M; AE P; AE Q; AE T; AE U; AE V; Tr. 129-130.

[24]Tr. 42-47.

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. . . ." An applicant has the ultimate burden of persuasion for obtaining a favorable security decision.

A person who seeks access to classified information enters into a fiduciary relationship with the Government predicated upon trust and confidence. This relationship transcends normal duty hours and endures throughout off-duty hours. The Government reposes a high degree of trust and confidence in individuals to whom it grants access to classified information. Decisions include, by necessity, consideration of the possible risk an applicant may deliberately or inadvertently fail to protect or safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation as to potential, rather than actual, risk of compromise of classified information.

Section 7 of Executive Order 10865 provides that decisions shall be "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." *See also* EO 12968, Section 3.1(b) (listing multiple prerequisites for access to classified or sensitive information).

Analysis

Guideline K, Handling Protected Information

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."

AG ¶ 34 describes the disqualifying conditions that could raise security concerns. I have considered all the conditions, and the following are potentially applicable:

> (g) any failure to comply with rules for the protection of classified or other sensitive information; and
>
> (h) negligence or lax security habits that persist despite counseling by management.

On two occasions, Applicant failed to return two blank classified cards used to take pictures of classified information or materials to their secured box at the conclusion of her mission. On both occasions, Applicant obtained a blank classified card to use in her camera if she needed to take photographs of classified information or sites. She never took any photographs on these cards. Because the cards remained blank at all

times, and thus, contained no pictures, she did not fail to protect classified information or other sensitive information as required by this guideline and under the NISPOM.

The SOR cites NISPOM Sections 5-100 and 5-303, providing notice to Applicant of the allegations of security concern. Neither of these provisions describe handling of media, in this case a photographic card marked classified, which did not contain classified information, that do not contain classified information. The contractor's SOP 16-001 in paragraph 7 describes the process for signing out, using, storing, and signing in media used for classified images. However, the SOP does not define the term "classified media" or indicate when unclassified media becomes classified media. SOP 16-001, paragraph 7b(1) states, "Keep *positive* control of all classified media *at all times*." SOP 16-001, paragraph 7c(3) requires classified media to be signed in (and properly stored) at the conclusion of the mission. If Applicant was not in personal possession of "classified media" or that media was not stored in the safe at the conclusion of the mission, she was in technical violation her employer's SOP.

In April 2009, Applicant initially locked the blank classified card as required. During her photo shoot, she placed the card in her purse which was in her possession, giving her positive control over the card at all times. In April 2010, she properly locked the card in a blue bag, locked the blue bag in her briefcase, and locked the briefcase in her government car. She parked the car in secured government parking. These actions met the NISPOM criteria to reasonably foreclose the possibility of loss or compromise.

At some point, Applicant's office apparently decided that security would be improved if all media, classified and unclassified, were treated the same. I conclude that her handling of the classified card did not violate the NISPOM or the SOP because the media did not contain any classified images. Applicant believed that she violated the SOP by failing to maintain positive control or to properly store the media, and I will therefore assume the Government established AG ¶¶ 34(g) and 34(h).

The Handling of Protected Information guideline also includes examples of conditions that can mitigate security concerns. I have considered mitigating factors AG ¶ ¶ 35(a) through 35(c), and the following are potentially applicable:

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

In April 2009, Applicant started work at 3:00 a.m. and continued to work until 7:00 p.m. that evening, a 16-hour work day. By the end of the day, she was exhausted. These long work hours and work days are unusual, as she normally works 10 hours a day, and such work hours are not likely to recur. The second incident occurred, in part,

because Applicant's supervisor continued to give her work assignments, then would change his mind about the assignment. By retaining the photo card in her secured brief case, Applicant was prepared for her next anticipated assignment. The confusion of this day was out of the ordinary and not likely to recur. Applicant is very clear about her responsibilities towards safeguarding classified information and has a positive attitude towards the discharge of her security responsibilities. AG ¶¶ 35(a) and 35(b) apply, and the SOR allegations 1.a and 1.b are found in favor of Applicant. Even if the allegations are not mitigated under Guideline K, they are mitigated under the Whole-Person Concept, *infra*.

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 the disqualifying conditions that could raise security concerns. I have considered all the conditions, and the following are potentially applicable:

> (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 person may not properly safeguard protected 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 other government protected information:
> >
> > (2) disruptive, violent, or other inappropriate behavior in the workplace;
> >
> > (3) a pattern of dishonesty or rule violations; and,
> >
> > (4) evidence of significant misuse of Government or other employer's time or resources; and

(f) violation of a written or recorded commitment made by the individual to the employer as a condition of employment.

The record contains four disciplinary reports prepared on May 3, 2010 or May 4, 2010. These reports concern the security incident in April 2009, the time incident in January 2010, the security incident in April 2010, and the counseling session in May 2010. Each report provides a space for an employee to acknowledge receipt of the disciplinary report. Applicant's signature is not on any of these reports, and she denies knowledge of any formal disciplinary action for the incidents listed in three reports. She does not deny disciplinary action for the April 2010 incident where she failed to return a blank classified card to its proper secure storage box. The SOR incorrectly alleges that Applicant received these disciplinary reports, when she did not. The Government has not established this SOR allegation as written. Applicant admitted to the underlying conduct in each allegation. Thus, the Government has established in SOR allegation 2.a. that the underlying conduct shows a violation of company rules by Applicant.

Applicant specifically denied allegations 2.b and 2.c. In January 2010, (SOR ¶ 2.b) Applicant filled out her time cards improperly because of a lack of guidance from her supervisor. Applicant did not violate any rules, but acted in good aith after attempting to get guidance from her supervisor on recording her work time. A few days later, HR provided clearer guidance for recording employee time due to the emergency situation. While her record has been documented, HR does not consider this documentation a disciplinary action. Applicant's actions in January 2010 reflect an honest mistake, not an attempt to violate the rules. Allegation 2.b is found in favor of Applicant.

Management met with Applicant in May 2010 to determine if she had any questions about her April 2010 security incident. Management then instructed her and those in the meeting not to discuss her security incident with anyone, except senior management. These instructions are prospective. On its face, this employee disciplinary report does not reflect any misconduct by Applicant, only possible discipline for a future violation. There is no evidence that Applicant violated the counseling given her. SOR allegation 2.c, as written, incorrectly asserts that Applicant received an oral warning as a disciplinary action, for discussing her security violation. SOR allegation 2.c is found in favor of Applicant.

As for the allegation of a security violation in SOR ¶ 1.d, the employee discipline report indicates that the report was prepared because of a safety violation, not a security violation. Applicant admits receiving the ticket. She signed for the disciplinary report. Her failure to buckle her seatbelt is a rules violation.

Overall, the SOR allegations under Guideline E reflect a pattern of rules violation in the workplace and a failure to follow the employer's standard operating procedures for handling blank classified photo cards between August 2005 and April 2010. The Government has established its case under AG ¶¶ 16(d)(4) and 16(f).

The Personal Conduct guideline also includes examples of conditions that can mitigate security concerns. I have considered mitigating factors AG ¶ 17(a) through 17(g), and the following are potentially applicable:

> (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;
>
> (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;
>
> (e) the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress; and
>
> (f) the information was unsubstantiated or from a source of questionable reliability.

Applicant has taken full responsibility for the actual incidents alleged in the SOR, even though she has denied receiving disciplinary reports for many of the incidents. The safety violation is the only safety occurrence in 18 years of employment. Because of the infrequency of safety violations over the last 18 years by Applicant, there is little likelihood that similar violations will occur. She has mitigated the Government's security concerns as to SOR ¶ 2.d under AG ¶ 17(d).

Applicant's employer moved her to another media work area after the April 2010 incident. She continues to read the SOP provisions required for her work section, which keeps her current on her employer's procedures for handling classified information. After the incidents in August 2005 and in February 2006, Applicant made suggestions to management for simple changes to eliminate future problems. Computer formatting problems are common, especially when new systems are being implemented, and are easily resolved. In August 2005, following Applicant's suggestion, management developed a template to prevent formatting problems. In February 2006, again following Applicant's suggestion, management installed a secure safe to store sensitive information in the small office where Applicant had worked. Applicant proposed simple solutions to prevent future problems of the type she experienced, and management found her solutions acceptable. These particular problems have not occurred for Applicant again. The evidence of record indicates that steps have been taken to eliminate future problems for Applicant. AG ¶¶ 17(d) and 17(e) are partially applicable. Even if the allegations are not mitigated under Guideline E, they are mitigated under the Whole-Person Concept, *infra*.

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 an applicant's conduct and all relevant circumstances. The administrative judge should consider the nine adjudicative process factors listed at AG ¶ 2(a):

> (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.

Under AG ¶ 2(c), the ultimate determination of whether to grant eligibility for a security clearance must be an overall commonsense judgment based upon careful consideration of the guidelines and the whole-person concept. The decision to grant or deny a security clearance requires a careful weighing of all relevant factors, both favorable and unfavorable. In so doing, an administrative judge must review all the evidence of record, not a single item in isolation, to determine if a security concern is established and then whether it is mitigated. A determination of an applicant's eligibility for a security clearance should not be made as punishment for specific past conduct, but on a reasonable and careful evaluation of all the evidence of record to decide if a nexus exists between established facts and a legitimate security concern.

The evidence in support of granting a security clearance to Applicant under the whole-person concept is more substantial than the evidence in support of denial. In reaching a conclusion, I considered the potentially disqualifying and mitigating conditions in light of all the facts and circumstances surrounding this case. Applicant has worked as a photographer for many years. Until 2005, she performed her duties without any identifiable problems. Over the next almost five years, six incidents occurred, some of which are clear violations of workplace rules, even though the incidents in question did not result in a compromise of classified or proprietary information. The incidents are the result of carelessness and inattention to rules, which raises a question of whether Applicant is acting or can act responsibly in handling classified information.

Applicant acknowledges each incident and admits her actions. The information in the record provides troubling facts about the disciplinary reports and accompanying implications. In January 2010, confusion arose on how to charge work time when the base closed because of flooding. Her supervisor wrote a memorandum for the record, indicating that he counseled her because she improperly charged her time on January 22, 2010. After receiving guidance from HR, he gave her guidance on how to charge her time for that day, which she did. Management approved her revised time sheet on January 26, 2010. The letter from the HR deputy supports this version of the events.

Most base employees improperly charged their time for the base closure. In May 2010, after Applicant's second incident with a blank classified photo card, employee disciplinary reports were prepared and placed in Applicant's file without her knowledge. Her supervisor prepared a written oral warning claiming violation of work rules and dishonesty for reporting her time on two days, not one, in January 2010. This report information differs significantly from the memorandum for the record and letter from the HR deputy explaining the time-reporting problems. Three-and-one-half months after the incident, Applicant's supervisor expanded his version of the events in January connected to her time card for unexplained reasons. His January 25, 2010 memorandum for the record is contemporaneous to the incident and is credible. The employee discipline report is given less weight because of the lapse of time and the appearance that in hindsight, he attempted to create a record of prior disciplinary action.

Applicant understood in April 2009 that an incident report would be filed with security because she did not property return the blank classified photo card at the end of the day. She received an oral warning from her supervisor, but no further disciplinary action was taken. Applicant's supervisor prepared an employee disciplinary report concerning this incident on May 4, 2010, nearly 13 months after the incident and without Applicant's knowledge. When this incident occurred, he did not deem it necessary to prepare any disciplinary report. The timing of the preparation of this report raises questions about the legitimacy of the report and the lack of serious concern about this incident when it occurred. As with the previous late report, this report is given less weight because of the lapse of time and the appearance that Mr. D was attempting to create a record of prior disciplinary action when none had occurred.

Issuing a disciplinary report for possible prospective misconduct raises some questions about why management chose this action and the actual validity of the report for purposes of misconduct. Oral warnings are verbal and not written as in this case. Given that management does not allege misconduct by Applicant in the disciplinary report, the report is given little weight as evidence to the extent it contradicts Applicant's statement of facts.

Applicant signed a very broad Last Chance Agreement in May 2010 and has complied with its terms. She has a long and generally favorable employment history with her company, as well as during her 14 years of service in the Marine Corps. Her work performance is excellent, and her co-workers at the base consider her trustworthy. Even after the April 2009 and April 2010 incidents, her employer gave her performance awards, which show its confidence in her work. None of her references mentioned knowing that she had a problem with her security clearance or the reasons for her SOR. In light of the oral warning given to her May 2010 about not discussing her security incidents with others, Applicant exercised good judgment in choosing not to violate the warning given her by providing these individuals with this information.

After a complete and thorough review of all the evidence of record, I find that Applicant is not a security concern despite her past carelessness and inattentiveness. She is fully aware of her responsibilities and the impact of any misstep by her in the future.

Overall, the record evidence leaves me without questions or doubts as to Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude Applicant mitigated the security concerns arising under Guidelines K and E.

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 K:	FOR APPLICANT
Subparagraph 1.a:	For Applicant
Subparagraph 1.b:	For Applicant
Paragraph 2, Guideline E:	FOR APPLICANT
Subparagraph 2.a:	For Applicant
Subparagraph 2.b:	For Applicant
Subparagraph 2.c:	For Applicant
Subparagraph 2.d:	For Applicant
Subparagraph 2.e:	For Applicant
Subparagraph 2.f:	For Applicant
Subparagraph 2.g:	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 eligibility for a security clearance. Eligibility for access to classified information is granted.

MARY E. HENRY
Administrative Judge