DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	
----------	)	ISCR Case No. 11-10901
	)	
	)	
Applicant for Security Clearance	)	

Appearances

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

11/29/2013

Decision

WESLEY, Roger C., Administrative Judge:

Based upon a review of the pleadings, exhibits, and testimony, I conclude that Applicant did not mitigate the security concerns regarding her handling of protected information. Eligibility for access to classified information is denied.

Statement of Case

On December 21, 2012, the Department of Defense (DOD) issued a Statement of Reasons (SOR) detailing reasons why DOD adjudicators could not make the preliminary affirmative determination of eligibility for a security clearance, and recommended referral to an administrative judge to determine whether a security clearance should be granted, continued, denied, or revoked. 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 (AGs) implemented by DOD on September 1, 2006.

Applicant responded to the SOR on January 17, 2013, and requested a hearing. The case was assigned to me on August 14, 2013, and was scheduled for hearing on September 26, 2013. At hearing, the Government's case consisted of six exhibits (GEs 1-6). Applicant relied on one witness (herself) and one exhibit (AE A). The transcript (Tr.) was received on October 4, 2013.

Procedural Issues

Before the scheduling of the hearing, Applicant requested a hearing in lieu of proceeding on the written record. Department Counsel concurred with Applicant's request, and the proceeding was converted to a hearing.

Before taking evidence at the hearing, Applicant requested an amendment of her SOR response to admit paragraph 1.b and deny paragraph 1.a. For good cause shown, Applicant's amendment request was granted, and the changes were made by inter-lineation.

Summary of Pleadings

Under Guideline K, Applicant is alleged to have (a) knowingly in October 2008 stored a CD containing secret classified information in an unauthorized location for approximately one year, and then unknowingly stored the CD in another unauthorized location for approximately six months (in violation of National Industrial Security Program Operating Manual (NISPOM) 5220.22-M, Sections 5-100, 5-300, and 5-302) and (b) knowingly disposed of the CD in September 2009 in an unclassified container (in violation of National Industrial Security Program Operating Manual, DOD 5520.22-M, Sections 5-700, 5-705, and 5-708)

In her answer to the SOR, Applicant admitted the alleged actions covered by subparagraph 1.b without explanation. She denied the allegations covered by subparagraph 1.a as written and admitted to a modified version of the allegation that changed the date of the alleged incident to October 2007 and the storage of the CD to one unauthorized location instead of two locations as written. Applicant offered no other explanations in her response.

Findings of Fact

Applicant is a 55-year-old software engineer of a defense contractor who seeks a security clearance. The allegations covered in the SOR and admitted by Applicant are incorporated and adopted as relevant and material findings. Additional findings follow.

Background

Applicant married in April 1980 and has two children from this marriage. (GE 1) Applicant claims no military service. She earned a bachelor's degree and earned a master's degree in December 1991 from a recognized university in her state. (GE 1)

Applicant worked for her current employer for several years before leaving the company in 1988. (Tr. 42) She returned to her employer in 1992 and has remained in its employ for a total of 30 years of combined employment. (GE 1; Tr. 36, 42-43)

Applicant's storage and destruction of classified information

In October 2007, Applicant was in her company's lab testing a classified radar model (classified secret) loaded on a CD (that was written by an engineer employed by another defense contractor. (GEs 3 and 4; Tr. 40) This engineer had suggested the need to test the model. On this testing day, Applicant and the engineer had returned from the lab with the CD containing secret classified information and attempted to find the right employees with the combination to the designated safe to open it and return the CD. (Tr. 40) Told that the two persons with the combination to the safe were out to lunch, Applicant attempted to find others to open the safe. (Tr. 40)

When Applicant was unable to locate another person to open the safe, she questioned another engineer at the site to ascertain what to do. (Tr. 40) This engineer suggested that since they were in a closed classified area, "it would be acceptable to put the disk in my [your] desk until they returned, which was expected to be before the end of the day." (Tr. 40) Following this engineer's suggestion, Applicant placed the CD in her desk, intending to return to the area before the end of the day to return the CD to the approved safe. (GE 4; Tr. 40)

Applicant never returned to the classified area to account for the CD she left in her desk, and forgot about it. (GE 4; Tr. 40, 47) She never performed any additional testing on the radar model covered by the CD she stored in her desk and was never asked about it by security personnel over the course of the ensuing year.

In October 2008, Applicant was in the process of packing up her belongings in anticipation of a move to another building when she located the CD in the desk drawer. (GE 2) Not sure of what actions to take with the disk, she left it in the desk drawer while she was figuring out what to do with the CD. (GE 2) Well-briefed with prior security training and refresher courses, Applicant was aware that her desk was not a designated area for storing the CD, and afraid to report her retention of the disk, she left the CD in her desk drawer while she contemplated what steps to take. (GE 2; Tr. 40-41, 66)

When Applicant once again located the missing classified CD in the spring of 2009 while cleaning out her desk, she panicked (afraid she could go to prison for her actions) and knowingly disposed of the CD in an unclassified LMAC proprietary information destruction container located near her work station. (GEs 3 and 4; Tr. 40-41) For over two years after disposing of the CD, she filed no reports with her employer's facility security officer (FSO) and remained silent about her actions. By the time an investigator inquired of Applicant in the spring of 2010 about the CD, she could not recall working on a classified radar model and told the investigator nothing about the CD. (GE 4; Tr. 41-42)

In April 2011, an investigator from Applicant's company asked her about the lost classified CD. Unable to recall working on the radar model, she told the investigator nothing. (Tr. 41) After surviving several sleepless nights trying to recall any work she might have performed on the radar model, she remembered the incident. (Tr. 41) At this time, she elected to self-report the incident to her FSO. (Tr. 41-42)

Upon learning of Applicant's 2009 handling of the CD in question, Applicant's FSO suspended her clearance pending further investigation. (Tr. 42-43) In a culpability report filed by a field office chief of the Defense Security service (DSS) in May 2011, the reporting official summarized the events covered by Applicant's self-report and concluded that the reported security violations were caused by Applicant's failure to follow known security practices and requirements. (GE 4) The DSS's field director, in turn, requested interim suspension of Applicant's security clearance pending further review. (GE 4) Following his field director's recommendation, DSS's director suspended Applicant's security clearance in June 2011, pending a final clearance decision from DOHA. (GE 4)

NISPOM guidelines

NISPOM guidelines impose responsibility on contractors for safeguarding classified information in their custody or under their control. (GE 5, Sec. 5-100) In turn, contractors that store classified material shall establish a system of security checks at the close of each working day to ensure that all classified material and security repositories have been appropriately secured. (GE 5, Sec. 5-102(a)) Contractors working multiple shifts must perform security checks at the end of the last working shift "in which classified material was removed from storage for use." (GE 5, Sec. 5-102(b))

Cognizant security officials (inclusive of software users like Applicant) must work to meet appropriate security needs according the intent of the NISPOM and at acceptable costs. (GE 5, Sec. 5-300) Secret material, in turn, shall be stored in a "GSA-approved security container, an approved vault, or a closed area" with supplemental controls. (GE 5, Sec. 5-303) These storage requirements directly covered Applicant and bound her to use utmost care in ensuring that classified CDs like the one she checked out was properly accounted for and properly stored at all times while under her control.

By Applicant's accounts of her storing of the CD in issue, she failed to follow NISPOM-approved storage procedures. While it is not clear whether she could keep the CD in her desk drawer while she remained in the secured area housing the desk, she was clearly required to return the CD to the appropriate safe once she departed the area. Applicant acknowledged as much and attributed her failure to secure the disk to prolonged memory loss. Her actions reflect negligent mishandling of the CD under all of the circumstances considered, but not deliberate disregard of established NISPOM storage procedures.

Destruction of classified materials are covered in detail by the NISPOM. Section 5-700 sets general requirements for the destruction of classified information. (GE 5) More specifically, classified material may be destroyed by burning, shredding, pulping, melting,

mutilation, chemical decomposition, or pulverizing. *See* Sec. 5-705 of NISPOM. Placement of a classified CD in a contractor's proprietary bin for destruction is not an approved destruction method. For classified waste covering test models no longer operational, persons in control of such materials are required to complete destruction of the material "as soon as practical." Sec. 5-708 of NISPOM. Pending destruction, persons holding the materials must safeguard the materials in accordance with governing guidelines for the level of classified materials involved. *See id*.

By at least October 2008 when she discovered the whereabout of the CD in issue in her desk drawer, Applicant was on notice of her mishandling of the CD, and was duty-bound at that point to notify her FSO of her actions. Instead, she left the CD in her desk drawer and outside of the designated safe while she considered what to do about her missteps.

By spring 2009, Applicant became aware once again of her continued storage of the CD in her desk drawer and the interest of FSO personnel in the whereabouts of the disk. Worried about reprimands and potential punishment, she panicked at this point and disposed of the CD in an unapproved proprietary bin. Not until April 2011 (some two years later) did she determine it was in her best interests to come forward and self-report her history of mishandling and disposing of the missing disk. Her employer responded with the interim suspension of her clearance, pending a further investigation of the reported incident.

Endorsements

Applicant is highly regarded by her supervisor, former manager, and colleagues who have worked with her for many years. Friends recognized her strong commitments to her family and church, and to her local civic and charitable communities. (AE A; Tr. 38-39) They describe her as a consistently organized, caring, honest, and trustworthy person who routinely adheres to high ethical standards when making value choices. (AE A) Colleagues and former managers characterize her as a well-respected technical leader in software development who is conscientious and dedicated in her work. (AE A) They cite her deep remorse for her mistake and support the reinstatement of her security clearance. (AE A) Applicant's supervisor credited her with recognition of her mistake and possession of qualities of strong moral and ethical behavior. (AE A) He believed she should be given a second chance and an opportunity to obtain a security clearance. (AE A)

Over the course of her 30-year tenure with her employer, Applicant has received consistently good ratings. She has also received monetary rewards on five occasions in the past 12 years in recognition of her contributions to her employer's missions. (Tr. 37)

Policies

The AGs list guidelines to be used by administrative judges in the decision-making process covering DOHA cases. These guidelines take into account factors that could

create a potential conflict of interest for the individual applicant, as well as considerations that could affect the individual's reliability, trustworthiness, and ability to protect classified information. These guidelines include "[c]onditions that could raise a security concern and may be disqualifying" (disqualifying conditions), if any, and many of the "[c]onditions that could mitigate security concerns."

These guidelines must be considered before deciding whether or not a security clearance should be granted, continued, or denied. The guidelines do not require administrative judges to place exclusive reliance on the enumerated disqualifying and mitigating conditions in the guidelines in arriving at a decision. Each of the guidelines is to be evaluated in the context of the whole person in accordance with AG ¶ 2(c).

In addition to the relevant AGs, administrative judges must take into account the pertinent considerations for assessing extenuation and mitigation set forth in AG ¶ 2(a) of the revised AGs, which are intended to assist the judges in reaching a fair and impartial commonsense decision based upon a careful consideration of the pertinent guidelines within the context of the whole person.

The adjudicative process is designed to examine a sufficient period of an applicant's life to enable predictive judgments to be made about whether the applicant is an acceptable security risk. The following AG ¶ 2(a) factors are pertinent: (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 chances; (7) the motivation for the conduct; (8) the potential for pressure, coercion, exploitation, or duress; and (9) the likelihood of continuation or recurrence.

Viewing the issues raised and evidence as a whole, the following individual guideline is pertinent in this case:

Handling Protected Information

> *The Concern*: Deliberate or negligent failure to comply with rules and regulations for protecting classified or other sensitive information raises doubt about and individual's trustworthiness, judgment, reliability, or willingness and ability to safeguard such information, and is a serious security concern. (AG ¶ 33)

Burden of Proof

By virtue of the principles and policies framed by the AGs, a decision to grant or continue an applicant's security clearance may be made only upon a threshold finding that to do so is clearly consistent with the national interest. Because the Directive requires administrative judges to make a commonsense appraisal of the evidence

accumulated in the record, the ultimate determination of an applicant's eligibility for a security clearance depends, in large part, on the relevance and materiality of that evidence. *See United States, v. Gaudin,* 515 U.S. 506, 509-511 (1995). As with all adversarial proceedings, the judge may draw only those inferences which have a reasonable and logical basis from the evidence of record. Conversely, the judge cannot draw factual inferences that are grounded on speculation or conjecture.

The Government's initial burden is twofold: (1) it must prove by substantial evidence any controverted facts alleged in the SOR, and (2) it must demonstrate that the facts proven have a material bearing to the applicant's eligibility to obtain or maintain a security clearance. The required materiality showing, however, does not require the Government to affirmatively demonstrate that the applicant has actually mishandled or abused classified information before it can deny or revoke a security clearance. Rather, the judge must consider and weigh the cognizable risks that an applicant may deliberately or inadvertently fail to safeguard classified information.

Once the Government meets its initial burden of proof of establishing admitted or controverted facts, the evidentiary burden shifts to the applicant for the purpose of establishing his or her security worthiness through evidence of refutation, extenuation, or mitigation. Based on the requirement of Exec. Or. 10865 that all security clearances be clearly consistent with the national interest, the applicant has the ultimate burden of demonstrating his or her clearance eligibility. "[S]ecurity-clearance determinations should err, if they must, on the side of denials." *See Department of the Navy v. Egan,* 484 U.S. 518, 531 (1988).

Analysis

Applicant is senior software engineer with many years of experience in accessing classified information without incident, who in 2007 knowingly stored a classified CD she was working on in a desk drawer outside of her employer's approved storage safe. After forgetting about her leaving the CD in her desk, she discovered the CD in her desk drawer a year later while preparing a move.

After noting its presence in her desk drawer, Applicant kept the disk in her drawer for another six months without alerting her superiors or FSO before locating it again and discarding it in a proprietary bin not approved for classified information destruction. Applicant's cited mishandling of the CD in issue reflects multiple incidences of mistaken decision-making, negligence, and faulty judgment and raises Government security concerns about her level of judgment, reliability, and trustworthiness.

The importance of safeguarding classified information cannot be overemphasized. Protecting the nation's security interests against the risks of foreign coercion and intimidation remains a core governmental responsibility that finds roots in the early federalist papers (*e.g., Federalist No. 8 (Hamilton)*, "Safety from external danger is the most powerful director of national conduct. Even the ardent love of liberty will, after a time, give way to its dictates") and enjoys the sustaining force of the courts.

Cf. United States v. Curtiss-Wright Corp., 299 U.S. 304, 319-20 (1936). Or put in geopolitical terms, national security policy implies a state of continuing readiness to take the necessary steps to maintain our national independence. *Cf.* H. Lasswell, *National Security and Individual Freedom* 51 (1950, reprinted 1971). What is to be weighed in this case are the actions of Applicant in her administering to the security requirements imposed by the NISPOM guidelines for protecting the classified CD entrusted to her custody and control.

By not reporting her storage of the missing CD before discarding it in an unapproved container, Applicant deliberately placed classified information in her custody and control at risk to compromise. Thereafter, her actions escaped scrutiny until she self-reported them to her company officials in April 2011. Her self-reporting actions resulted in her company's initial suspension of her clearance and its referral of its findings to DSS for further review.

Under the NISPOM's security guidelines in force, persons responsible for safeguarding classified information in their custody and control are required to keep the materials secured in designated areas and to avoid taking classified materials outside the designated area, destroying them in unapproved ways, or mishandling them in their work sites. Responsible individuals like Applicant who either initially misplace a CD containing classified information, or fail to undertake known appropriate storage measures before departing a classified area, are required to immediately notify their security manager or superiors. Security violations are, in turn, treated most seriously and are considered to reflect negatively on a person's continued eligibility for security clearance and access to classified information.

Moreover, although the classified CD in issue was never compromised nor misappropriated in any manifest ways, Applicant committed several security violations in storing the CD in an unauthorized desk drawer and then destroying it in a unauthorized proprietary bin without disclosing her actions to her FSO or superiors for their approval. Whether or not the copied classified disk was ever compromised or not, Applicant's actions were undertaken negligently initially and then compounded by her knowingly and wilful destruction of the disk in an unapproved manner. Her collective actions constituted violations of NISPOM security guidelines and placed known classified material at risk to compromise.

As a contractor fiduciary with access to classified materials, Applicant was duty-bound to exercise not only personal accountability over her assigned safeguarding responsibilities, but prudent reporting of any potential security breaches as well. Holding a personal security clearance and having eligibility for access to classified information draws upon the highest fiducial burdens imposed on persons with access to facilities covered by the NISPOM guidelines and enables the Government to rightfully insist on a clearance holder's close adherence to governing trust responsibilities.

Applicant, as a lead software engineer for her technical team and a fiduciary of entrusted classified materials can and should be held accountable for security violations that derive from her knowing and willful mishandling of classified materials. *See* ISCR

Case No 07-08119 at 5 (App. Bd. July 8, 2010); ISCR Case No. 04-04264 at 3 (App. Bd. Sept. 8, 2006); ISCR Case No. 89-0781 (February 23, 1993). Her actions invite application of DC ¶ 34(b), "collecting or storing classified or other protected information at home or in any other unauthorized location," and DC ¶ 34(g), "any failure to comply with rules for the protection of classified or other sensitive information." The AGs for handling protected information are clearly reconcilable with the storage and destruction guidelines in the NISPOM for handling classified materials in the clearance holder's custody and control.

By improperly storing the classified CD in a non-approved desk outside the designated safe for a prolonged period without reporting her findings, and later destroying the disk in an unapproved proprietary bin without any approvals from her FSO or superiors, Applicant showed considerable neglect and material disregard for protecting classified information in her custody and control. Because Applicant's actions reflect judgment lapses and a disposition to conceal her efforts, Guideline K's core security concerns of trustworthiness, judgment, reliability, and willingness to safeguard classified information come into play. *See* ISCR Case No. 00-0030 at 7 (App. Bd. Sep. 20, 2001).

In appraising the security significance of Applicant's security violations, careful consideration was given to Applicant's clean record preceding the incident under review, her standing with her company, and her positive contributions to her company, family, church, and civic community. Applicant's explanations of her mishandling the classified CD in her possession and control are insufficient to extenuate and mitigate the security violations attributable to her.

Based on Applicant's own experience and security training and the seriousness of her (a) failing to properly store the classified CD after she departed the safe area; (b) her failure to report her findings once she became aware of the CD's whereabouts a year later; and (c) her improper destruction of the CD without disclosing her actions to her FSO or superiors in a timely way, Applicant may not take full advantage of three of the mitigating conditions under the guidelines for security violations. Neither MC ¶ 35(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;" MC ¶ 35(b), "the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities;" nor MC ¶ 35(c), "the security violations were due to improper or inadequate training," are fully applicable to Applicant's situation.

In fairness to Applicant, she has no prior history of security violations, and she has exhibited remorse and renewed understanding about the importance of protecting classified information in her custody and control. Both her contributions to her employer, church, and civic community, and her attitudinal changes are acknowledged, and for

this she is to be both commended and encouraged. It is too soon, however, to conclude that Applicant has successfully mitigated the actions attributable to her.

So, while the cited mitigating conditions have some applicability based on Applicant's unblemished history of handling classified information, her expressed remorse, and the favorable recommendations from her friends, colleagues, supervisor and former manager, these positive influences and considerations are not enough to mitigate her actions. More time is needed to mitigate Applicant's actions associated with her mishandling of classified information in her possession and control under the facts and circumstances covered in this record. Considering all of the evidence, Applicant does not at this time carry her evidentiary burden in demonstrating her eligibility to access classified information.

In making a whole-person assessment, careful consideration was given to the respective burdens of proof established in *Egan* (*supra*), the AGs, and the facts and circumstances of this case in the context of the whole person. Unfavorable conclusions warrant with respect to the allegations covered by Guideline K.

Formal Findings

In reviewing the allegations of the SOR and ensuing conclusions reached in the context of the findings of fact, conclusions, conditions, and the factors listed above, I make the following formal findings:

GUIDELINE K (Handling Protected Information): AGAINST APPLICANT

Subparas. 1.a and 1.b: Against Applicant

Conclusions

In light of all the circumstances presented by the record in this case, it is not clearly consistent with the national interest to grant or continue Applicant's security clearance. Clearance is denied.

Roger C. Wesley
Administrative Judge