DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 10-01648
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: D. Michael Lyles, Esq., Department Counsel
For Applicant: *Pro se*

March 24, 2011

Decision

RICCIARDELLO, Carol G., Administrative Judge:

Applicant mitigated the Government's security concerns under Guidelines K, Handling Protected Information, and Guideline M, Use of Information Technology Systems. Applicant's eligibility for a security clearance is granted.

Statement of the Case

On September 10, 2010, the Defense Office of Hearings and Appeals (DOHA) issued Applicant a Statement of Reasons (SOR) detailing security concerns under Guidelines K and M. 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 (AG) effective within the Department of Defense on September 1, 2006.

Applicant answered the SOR on October 22, 2010, and requested a hearing before an administrative judge. The case was assigned to me on January 13, 2011.

DOHA issued a Notice of Hearing on February 9, 2011. I convened the hearing as scheduled on March 1, 2011. The Government offered Exhibits (GE) 1 through 8. Applicant did not object and they were admitted into evidence. Applicant testified on his own behalf, and offered Exhibits (AE) A through D. Department Counsel objected to AE A and D. His objections were overruled and AE A though D were admitted into evidence. DOHA received the hearing transcript (Tr.) on March 8, 2011.

Findings of Fact

Applicant denied the SOR allegations in ¶¶ 1.a, 1.b, and 1.c, and did not admit or deny the sole allegation in ¶ 2.a. After a thorough and careful review of the pleadings, exhibits, and testimony, I make the following findings of fact.

Applicant is 31 years old. He earned a bachelor's degree in 2002 and a master's degree in 2004. He began working for his present employer in 2004, after he completed his master's degree. He is not married and has no children. He was granted an interim secret security clearance in 2004 and, in 2005, he was granted a full clearance.

In December 2004, while holding an interim secret security clearance, Applicant performed a "trusted document download" program on an unclassified system and failed to accurately reference the security classification guide. He subsequently downloaded classified information he thought to be unclassified onto the company's Wide Area Network (WAN).[1]

Applicant explained that he had only recently graduated from his master's program and was new to the company. He explained that he had followed the proper procedures in using the "trusted download" program. The program is supposed to detect and black out any classified words contained in the document, so a redacted classified document can be downloaded onto an unclassified system. Applicant indicated that he spent a month referencing the security labels on the database and checked the data to ensure it did not include classified material. His coworkers assisted him in the process and agreed the information was cleansed. He went through the document line by line ensuring there was no classified information. He followed the prescribed protocol. He then emailed the data as an attachment and a team member looked at the data and pointed out that there was a combination of two words, that when juxtaposed, were considered classified. Each of the two words, when they stood alone, was not considered classified. The "trusted download" program did not detect the two words.[2]

Applicant's supervisor had discussions with five others to determine whether the words were classified. Three of those it was referred to were security officers, the fourth held a top secret security clearance, and the fifth was the program manager. After a day of discussions with others in the company, the supervisor deferred the decision to the program manager who ultimately chose to err on the side of caution and labeled the

[1] Tr. 37-39, 90-92.

[2] Tr. 37-45, 83-87; GE 6.

words classified. In doing so, it was determined Applicant violated the rules of protecting classified information and received a written reprimand. Applicant stated that whoever classified the words did not note the distinction of using the words separately and together. He explained that it was not until an experienced person, who held a higher security clearance, reviewed the information, that the subtlety was noted. Applicant believed he took precautions and he complied with the rules. He had attended security training and asked people to review his work prior to transmitting the data electronically. Upon discovery, proper procedures were followed to cleanse and sanitize the affected hardware. The possibility that classified material was lost or unaccounted for could not be precluded. Applicant no longer performs "trusted downloads" on any system because he concluded it is not reliable. He advised others not to use it also. He no longer accepts an assignment that tasks him with sanitizing classified data so the document can be viewed on an unclassified system.[3]

On January 4, 2005, Applicant was the last person to leave a secure area where he worked. It was the responsibility of the last person in the space to follow proper security procedures before leaving. In addition to ensuring all computers were turned off and documents were secure, the last person was required to make a log entry stating the time he or she left, and verify the spaces were secure. It also required that the last person remaining secure the lock by spinning it to make sure it was locked properly. Applicant was the last person to leave and failed to spin the lock because he became distracted by a telephone call prior to leaving. It was determined that the space was unlocked for approximately 18-20 minutes before the security guards noted the discrepancy. Applicant admitted he failed to spin the lock. The space is a secure room that requires three security procedures to enter. First, an employee must swipe their badge. Second, the employee enters a personal security code into a phone pad. Third, the employee opens the door using the combination lock. Throughout the day, the door does not require the lock to be spun, but at night the last person needs to secure the lock. Because others had also failed to adhere to the specific requirements to secure the spaces, new procedures were implemented that required at least two people to jointly secure the spaces at night.[4]

Applicant was reminded after the incident how to properly secure the lock and of his responsibility to properly protect classified information and exit closing procedures. He was also required to attend a Closed Area Briefing. It was determined that a compromise of classified information did not occur. Because this was a second security infraction within a year, Applicant was suspended from work for five days without pay.[5]

In August 2009, as part of his work responsibilities, Applicant provided detailed feedback to a deployed technology group that develops the technology used by his company. The deployed technology group had a higher level of classification than

[3] Tr. 37-45; GE 2, 6; Answer to SOR.

[4] Tr. 45-51, 65-68; GE 2, 6; Answer to SOR.

[5] Tr. 51; GE 7; Answer to SOR.

Applicant. He gave them feedback on a "mechanism" through the unclassified email system. Applicant explained that because the "mechanism" was "obvious and visible" he did not believe mentioning the "mechanism" was classified. The "mechanism" is in the classification guide and it is classified. Applicant stated he spoke with his coworkers before he sent the email using the "mechanism" name. The security investigation determined that classified information was transmitted over unsecured networks and it must be assumed that a compromise of the classified information occurred. It determined that Applicant's interpretation of the "mechanism" being "obvious and visible" was broader than it should have been. Applicant did not believe he was transmitting classified information. A supervisor with a top secret security clearance, who worked on special access programs, determined Applicant made an incorrect interpretation. Applicant was cited for a security violation and given a written reprimand. The investigation determined that Applicant's conduct was not deliberate.[6]

Applicant acknowledged his mistakes and takes the matters very seriously. He has become a champion of following all security rules and regulations. After the first incident he took a refresher course in handling classified information. He also read classification guides and other guidance on computer-related classifications. As a lead engineer, he repeatedly reinforces to his subordinates the importance of absolute compliance. He has implemented new procedures to correct flaws he observed in the security system. He has drastically curtailed providing detailed feedback on unclassified systems, which was the cause of the last incident. This has slowed down technical development because he now uses a classified system for his feedback. Applicant has participated in additional operational security training. He emphasizes the importance of security everyday and has talked to his coworkers about the violations he committed and the importance of adhering to all the rules. He recommends they always have two people review their work before sending information out on an unclassified system.[7]

Applicant provided character letters from coworkers. They attest to his attention to detail, dependability, resourcefulness, and good attitude. His technical skills are unmatched, and he is a mentor to new engineers. One letter mentions that Applicant has taken additional classes and read material to ensure he adheres to Operational Security and Classification Requirements. Applicant received an award for his substantial contributions to the company's goals. A coworker explained how Applicant has used his own security problems to warn others to be diligent and of the hazards that can arise in a secure environment. He is known to take extra precautions to ensure all security rules and regulations are adhered to. He is considered an honest man with integrity.[8]

[6] Tr. 51-63, 68-83, 87-90; GE 2, 8; Answer to SOR.

[7] Tr. 92-101.

[8] Tr. 63-64; AE A.

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. Likewise, I have avoided drawing inferences grounded on mere speculation or conjecture.

Under Directive ¶ E3.1.14, the Government must present evidence to establish controverted facts alleged in the SOR. Under Directive ¶ E3.1.15, an "applicant is responsible for presenting witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by applicant or proven by Department Counsel and has the ultimate burden of persuasion to obtain a favorable security decision."

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 the applicant may deliberately or inadvertently fail to safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation of 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, Handing 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 conditions that could raise a security concern and may be disqualifying. The following are potentially applicable.

> (c) loading, drafting, editing, modifying, storing, transmitting, or otherwise handling classified reports, data, or other information on any unapproved equipment including but not limited to any typewriter, word processor, or computer hardware, software, drive, system, gameboard, handheld, "palm" or pocket device or other adjunct equipment;
>
> (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.

Applicant committed security violations in 2004, 2005, and 2009. He received a written reprimand in 2004. He was suspended without pay in 2005 and attended additional training. In 2009, he received a written reprimand. I find the above disqualifying conditions apply.

The guideline also includes conditions that could mitigate security concerns arising from handing protected information. I have considered the following mitigating conditions under AG ¶ 35:

> (a) so much time has elapsed since the behavior, or it has happened so infrequently or under such unique circumstances that it is unlikely to recur and does not cast doubt on the individual's 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 was new at his job in 2004. He took all necessary precautions when he used a "trusted download" program to cleanse a classified document. He followed the proscribed protocol. He asked his coworkers to assist him in the process and confirm it was cleansed. It was only later, when a more experienced supervisor scrutinized the document and sought advice from others, that it was determined the document had two words that were unclassified when used separately, but classified when they were juxtaposed. Applicant was reprimanded for his actions.

Applicant admitted that in 2005 he failed to spin the lock to secure the spaces where he worked. A new two-person procedure has been implemented to prevent recurrence. In 2009, Applicant believed he was acting properly when he referred to a "mechanism" on an unsecure network. He asked for guidance from his coworkers before using the term. The term was included in the classification guide.

Although Applicant committed security violations in 2004 and 2009, they appear to be the result of improper or inadequate training. He asked for assistance, sought guidance, scrutinized the protocol and documents, but ultimately he was held accountable when it was later determined that his analysis was wrong. I find AG ¶ 35(c) applies.

The violation that occurred in 2005 was due to Applicant's negligence when he became distracted and failed to secure the office properly. Because this was a recurring problem in the office a new procedure was implemented. Applicant acknowledges his mistakes. He has become a champion of following all security rules and regulations. As a lead engineer, he repeatedly reinforces to his subordinates the importance of absolute compliance. He has implemented new procedures to correct flaws he observed in the security system. He has drastically curtailed providing detailed feedback on unclassified systems, which was the cause of the last incident. He has participated in additional operational security training. He emphasizes the importance of security everyday and has talked to his coworkers about the violations he committed and the importance of adhering to all the rules. He recommends they always have two people review their work before sending information out on an unclassified system. I find the 2004 and 2009 incidences happened under unusual circumstances. I find with Applicant's renewed commitment to security awareness that future incidences are unlikely to recur.

I also find with regard to all three violations that they do not cast doubt on Applicant's current reliability, trustworthiness, or good judgment. He has responded favorably to counseling and security training and now demonstrates a positive attitude toward the discharge of his security responsibilities. I have considered that Applicant was attempting to do the right thing in 2004 and took precautions to ensure he was acting correctly. Again in 2009, he believed he was acting appropriately and was taking precautions. Unfortunately, he was wrong. He has since changed the way he conducts himself and has reinforced his commitment to properly handling classified information. The 2005 violation was the only one that was due to his negligence. I find AG ¶¶ 35(a) and 35(b) apply.

Guideline M, Use of Information Technology Systems

AG ¶ 39 expresses the security concern pertaining 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 reliably 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.

AG ¶ 40 describes conditions that could raise a security concern and may be disqualifying. I have especially considered the following:

> (d) downloading, storing, or transmitting classified information on or to any unauthorized software, hardware, or information technology system; and
>
> (g) negligence or lax security habits in handling information technology that persists despite counseling by management.

Applicant committed two security violations involving information technology from 2004 to 2009, as detailed above. I find the above disqualifying conditions apply.

I have considered all of the mitigating conditions under AG ¶ 41 and especially considered the following:

> (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;
>
> (b) the misuse was minor and done only in the interest of organizational efficiency and effectiveness, such as letting another person use one's password or computer when no other timely alternative was readily available; 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 supervisor.

The same analysis as discussed above applies to this guideline. The violations committed by Applicant in 2004 and 2009 can be attributed to his inexperience. Despite his effort to comply with the rules, his analysis was wrong. As detailed above, he has

committed himself to a new level of security awareness. I find AG ¶¶ 41(a) and 41(c) apply. I find there in insufficient evidence to find AG ¶ 41(b) applies.

Whole-Person Concept

Under the whole-person concept, the administrative judge must evaluate an applicant's eligibility for a security clearance by considering the totality of the applicant's conduct and all the 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.

I considered the potentially disqualifying and mitigating conditions in light of all the facts and circumstances surrounding this case. I have incorporated my comments under Guidelines K and M in my whole-person analysis. Some of the factors in AG ¶ 2(a) were addressed under those guidelines, but some warrant additional comment.

Applicant is a well respected employee. He is considered a hard worker and a person of integrity. He committed three security violations in six years, the last occurring in 2009. Despite his efforts to do things correctly, he made errors. Applicant has committed himself to ensure he is cautious and complies with all security rules and regulations. I believe Applicant was acting in good faith and relied on the assistance and advice of others in 2004 and 2009. I do not believe Applicant is a security risk. Overall, the record evidence leaves me with no questions or doubts about Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude Applicant successfully mitigated the security concerns arising under Guideline K, Handling Protected Information and Guideline M, Use of Information Technology Systems.

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
Subparagraphs 1.a-1.c:	For Applicant
Paragraph 2, Guideline M:	FOR APPLICANT
Subparagraph 2.a:	For Applicant

Conclusion

In light of all of the circumstances presented by the record in this case, it is clearly consistent with the national interest to grant Applicant a security clearance. Eligibility for access to classified information is granted.

_____
Carol G. Ricciardello
Administrative Judge