DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 09-00906
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Alison O'Connell, Esquire, Department Counsel
For Applicant: William Bransford, Esquire, and Christopher J. Keeven, Esquire

July 29, 2010

Decision

ANTHONY, Joan Caton, Administrative Judge:

After a thorough review of the case file, pleadings, testimony, and exhibits, I conclude that Applicant failed to mitigate the Government's security concerns under Guideline K, Handling Protected Information, Guideline E, Personal Conduct, and Guideline M, Use of Information Technology Systems. His eligibility for a security clearance is denied.

Applicant completed and signed a security clearance application (SF-86) on September 18, 2001. On December 14, 2009, the Defense Office of Hearings and Appeals (DOHA) issued Applicant a Statement of Reasons (SOR), detailing security concerns under Guideline K, Handling Protected Information, Guideline E, Personal Conduct, and Guideline M, Use of Information Technology Systems. 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 for SORs issued after September 1, 2006.

On December 22, 2009, Applicant answered the SOR in writing. He elected to have a hearing before an administrative judge. The case was assigned to me on March 29, 2010, and a notice of hearing was issued on March 31, 2010, setting Applicant's hearing for May 3, 2010. I convened the hearing, as scheduled, to consider whether it is clearly consistent with the national interest to grant or continue a security clearance for Applicant.

The Government called no witnesses and introduced seven documents. Six of the documents were marked Ex. 1 through 6 and admitted to the record without objection. The Government also provided military directives for administrative notice. The Government's administrative notice documents were marked as Hearing Exhibit (HE) 1. Applicant did not object to the administrative notice documents.

Applicant testified on his own behalf and called four witnesses. He introduced two exhibits, which were identified and marked as Exs. A and B. Applicant's exhibits were admitted without objection. DOHA received the transcript (Tr.) of the hearing on May 12, 2010.

Findings of Fact

The SOR contains three allegations of disqualifying conduct under Guideline K, Handling Protected Information; two allegations of disqualifying conduct under Guideline E, Personal Conduct; and one allegation of disqualifying conduct under Guideline M, Use of Information Technology Systems. Applicant admitted all allegations in the SOR. His admissions are admitted as findings of fact. (SOR; Answer to SOR.)

Applicant is 39 years old, married, and the father of four young children. Since August 2008, he has been employed by a government contractor. (Ex. 1; Tr. 26-27.)

Applicant attended college on an ROTC scholarship and received a Bachelor of Science degree in Aviation Management. Applicant was commissioned as a U.S. military officer and completed basic training before he resigned for health reasons. He worked in the private sector for about five and one-half years. He reentered the military in July 2000 and advanced to the rank of O-4. He deployed in 2008. He completed his required active service and was honorably separated from active duty in September 2008. During his military career, he served for over eight years as a logistics officer. (Ex. 1; Ex. 2 at 4; Tr. 27-29.)

In about February 2007, while serving as a military officer, Applicant was assigned to serve as a program officer and to direct a testing and evaluation program for a military application. Applicant was tasked with significant responsibilities and worked in an intense and stressful environment. He worked long hours and traveled frequently. During this time, he lived with his family on a U.S. military installation, where components of the testing and evaluation program were also located. (Tr. 29-32, 38-39, 73-75.)

As a part of his duties during this time, Applicant drafted a security classification guide for his program. In August 2007, on a Friday afternoon, Applicant was working in a secure facility on the base. He received an assignment to prepare a briefing on the status of two vendors in the testing and evaluation program for delivery the following Monday morning by the military official who directed the application program. Applicant knew that it would be necessary for him to acquire or access certain classified documents and photographs in order to complete the assignment. He also knew that to complete the assignment on time, it would be necessary to work over the upcoming weekend. All of the classified information that he needed to prepare the briefing could be accessed from the secure facility where Applicant worked. (Ex. 3 at 1; Tr. 32-35, 74-79, 109-110.)

Applicant, however, called a civilian contractor courier assigned to his program at an installation about two hours away by automobile and directed him to bring classified information, stored on computer disks, to him at the military base.[1] The information on the disks was accessible on the classified computer network available to Applicant at the base. However, Applicant believed that downloading classified material from the classified computer network would be slow and difficult. (Ex. 3 at 1-2; Tr. 73-74.)

When a courier transporting classified information arrived at the base, he or she would take the classified information to a secure command site, where it would be logged in by a military officer of the day and secured in classified storage. However, when the courier arrived at the base carrying the classified information requested by Applicant, Applicant directed him to take the classified information to his residence, which was located on the base approximately three to four miles from the secure facility where Applicant worked. (Ex. 3 at 2; Tr. 75, 110-111.)

At his residence, Applicant took possession of the classified computer disks from the courier. He told the courier he would not sign a chain of custody document when he received the classified materials. He acknowledged to the courier that he was breaking rules for the receipt and possession of classified information. He directed the courier not to tell anyone about his rule breaking. He then directed the courier to return to his residence the following day, Saturday, to retrieve the classified documents and return them to classified storage at the other installation. (Ex. 3 at 2; Tr. 74-77.)

On Friday evening, Applicant worked with the classified information at his kitchen table. He loaded the classified images and text onto his personal computer. He described his actions as follows:

> I took the CDs of the vendors---or the ones I needed to have the information from, and put them on to an “unclass computer.” It wasn’t hooked up to the Internet. It wasn’t turned on, wireless. You know, I couldn’t - - I used a personal computer [be]cause my [government-issued]

[1] The courier was assigned to the program that Applicant directed. Applicant testified that he had the authority to give the courier tasks and assignments. (Tr. 136-139.)

> laptop wasn't working correctly to copy. I copied those videos, put all the CDs back together, burned the new disk, deleted everything off my computer, and everything back in the bag, and put it in my filing cabinet.

(Ex. 3; Tr. 80-81.)

As he worked on the classified materials at his kitchen table, his wife came into the room. On February 6, 2008, Applicant provided the following description in a sworn, signed statement to an authorized investigator:

> I admit that I did show my wife [name omitted] some clearly marked "Secret" videos that I had copied from the CDs to my personal laptop. I know she does not have any sort of clearance, nor is she a government employee or service member. She stopped by the table where I was working so I showed her a video and stated, "This is part of the program."

(Ex. 3 at 2.)

At his hearing, Applicant described the same event as follows:

> You know, I was sitting there, working, and, you know, my wife came around and said, "What are you working on?" I said, "I'm working on- - trying to get this done for work, and - - and a video was playing at the same time, and I said, "This is my work." She said, "Oh, okay," and off she went.

(Tr. 81.)

At his hearing, Applicant denied deliberately showing his wife a classified video. He stated that he was playing a classified video as a part of his work, and his wife happened to see it as she came into the kitchen and asked about the work he was doing. He replied to his wife's question by identifying the video as a part of his work. (Tr. 114-116.)

Applicant was tasked with preparing a classified briefing and unclassified materials that could also be distributed. As he prepared the briefing, Applicant had access to unclassified photographs of the application that had previously been distributed. As he reviewed the classified photographs on the videos he was using to prepare the classified briefing, Applicant decided that some of the photographs designated as classified had been mismarked. Applicant then cropped the classification markings from the classified pictures so that they could be put on an unclassified computer network (NIPERnet) and cleared for distribution. He testified that he did not have classification authority; he also testified that he thought he had the authority to change the classified photographs to unclassified by removing the classified designation from the photographs. (Tr. 77-78, 117-120.)

On Friday evening, Applicant used the classified CDs to create smaller CDs containing the video and photographs of interest for the briefing. This process took about four hours. After completing this process, he deleted the files from his personal computer.[2] On Saturday, the contractor courier returned to Applicant's residence to retrieve the classified materials and return them to the secure site where they had been stored. (Ex. 3 at 2-3; Tr. 113-114.)

Applicant did not work on the briefing on Saturday. On Sunday, he went to the secure site on the base and used secure technology to assemble and complete the classified briefing. As a part of that process, he loaded images he created from the classified CDs he had placed on his unclassified personal computer onto the secure classified network (SIPRnet). He completed the assignment and provided the military official with the materials and information he had requested for the Monday morning briefing. (Tr. 84-85; 121-122.)

Applicant testified that as a military officer he had been trained in security processes and had worked extensively on the security classification guide for the application program for which he served as a testing and evaluation program officer. He stated that he knew the rules and knew he was breaking them. He also stated that he did not know he did not possess the authority to reclassify or declassify classified information until he took a basic information security independent study course in September 2009. (Ex. B; Tr. 85-86, 118-121.)

There were no immediate negative consequences to Applicant's actions in carrying out the briefing assignment. Sometime after the August 2007 incident, Applicant assigned the contract courier to a component unit in another part of the United States. At his new assignment, in about December 2008, the courier invited some other employees to look at some classified videos on his non-secure laptop computer. The other employees informed Applicant of the courier's actions, and Applicant reported the individual to the unit's security manager. When investigators questioned the courier, he told them that Applicant had authorized him to put the classified videos on his laptop computer. (Ex. 3 at 3; Tr. 87-88, 122-123.)

Applicant speculated that the videos the courier had on his laptop computer contained classified information that was on the CDs that he had brought to Applicant's residence in August 2007. He realized that because the courier had implicated him, he too would be questioned and his actions investigated. He drafted a statement about his actions in August 2007 that he gave to his program manager. He then met with his immediate supervisor and told him what he had done and how he had violated rules and regulations for protecting classified information. On November 30, 2007, Applicant's command was informed of his disregard for security requirements. As a consequence, Applicant's access to classified information was removed, his personal computer was

[2] Applicant described his actions as follows: "After I had completed downloading the [classified] marked photos and videos and burned them to two CD's, I went ahead and deleted the files, and then emptied the recycle bin on my personal computer. I thought the files were completely removed from my personal computer." (Ex. 3 at 2.)

confiscated for forensic analysis, and his actions were investigated by a military criminal investigation unit. (Ex. 7; Tr. 88-91, 122-124.)

The forensic analysis of Applicant's personal unclassified computer revealed the "fingerprint" of the classified files he copied to the computer when working in his residence in August 2007. Applicant stated that when he deleted the classified files, he did not understand that the fingerprint of the classified information remained on his personal computer. (Tr. 89-90.)

On May 5, 2008, Applicant's command conducted an Article 15 hearing into Applicant's conduct. Applicant received nonjudicial punishment for violation of a lawful general regulation (Article 92) and was issued a punitive letter of reprimand. His commander's report cited the following specific facts as determinative in the imposition of nonjudicial punishment: "Having access to materials classified as 'Secret,' [Applicant] violated a lawful general regulation . . . by improperly handling and storing classified material on his personal computer as he prepared an official brief for his command." (Ex. 6 a1; HE 1; Tr.39-40.)

Applicant asserted that he was confident that he would never violate security rules again. He discussed the lessons he had learned from his experience:

> Just, you know, shortcuts do not . . . save time. [L]ooking back, with the number of hours, you know, the disappointment, the regret . . . even my wife, who has . . . been aware of this for two and a half years now. . . [T]o look at such a poor decision, to derail a career, to save a half a day's work. I mean, it's just a reinforcement that you just can't take shortcuts . . . [I]f I could go back in time . . . with . . . hindsight, out of a million times I'd make the correct choice a million times over. And you know . . . it's been a lesson to me.

(Tr. 107-108.)

The SOR alleges a number of incidents that raised security concerns under Guidelines M, K, and E. Specifically, SOR ¶ 1.a. alleges, under Guideline K, that Applicant improperly handled and stored classified information between about August 11, 2007 until November 30, 2007, in violation of a lawful general military regulation, and, as a consequence of this violation, he received nonjudicial punishment under Article 92 of the Uniform Code of Military Justice (UCMJ). The SOR alleges that this conduct also raises security concerns under Guideline E and Guideline M (SOR ¶¶ 2.a. and 3.a.).

The SOR alleges at ¶ 1.b. that Applicant raised security concerns under Guideline K when, in 2007, he removed secret classification markings from classified photographs without authority so that he could move the classified photographs from a classified computer network to an unclassified computer network. The SOR alleges that

this conduct also raises security concerns under Guideline E and Guideline M (SOR ¶¶ 2.a. and 3.a.).

The SOR alleges at ¶ 1.c. that Applicant raised security concerns under Guideline K when, without authority, he showed classified material to his wife, who did not have a security clearance or a need to know the classified information. This conduct is also alleged as a security concern under Guideline E (SOR ¶ 2.a.).

The SOR alleges at ¶ 2.b. that Applicant raised a security concern under Guideline E when he instructed a contract employee to carry classified information to his residence in August 2007, when he knew that the instruction violated procedures for protecting classified information, and also instructed the individual not to tell anyone of the violation.

Applicant's former commanding officer, who presided at Applicant's Article 15 hearing, appeared as a witness on his behalf. He stated that Applicant performed his military duties very well. He also observed that it was his conclusion that Applicant did not intentionally pass classified material to anyone who should not have it. (Tr. 38-43.)

The president and vice president of the government contracting firm which employs Applicant also appeared as witnesses. The president stated that he had met and worked with Applicant when he was in the military, and he noted that Applicant has been employed by his firm for about two and one-half years. He considers Applicant to be a competent employee and a valued member of his team. The vice president praised Applicant's character as "outstanding." (Tr. 52-66, 167.)

Applicant's supervisor also appeared as a witness. He described Applicant's character as "top notch" and his work performance as "exemplary." (152-153.)

Policies

The U.S. Supreme Court has recognized the substantial discretion of the Executive Branch in regulating access to information pertaining to national security, and it has emphasized that "no one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988). As Commander in Chief, the President has the authority to control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to have access to such information." *Id*. at 527. The President has authorized the Secretary of Defense or his designee to grant Applicant's eligibility for access to classified information "only upon a finding that it is clearly consistent with the national interest to do so." Exec. Or. 10865, *Safeguarding Classified Information within Industry* § 2 (Feb. 20, 1960), as amended and modified.

When evaluating an applicant's suitability for a security clearance, an administrative judge must consider the revised adjudicative guidelines (AG). 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, the administrative judge applies these guidelines in conjunction with the factors listed in the adjudicative process. The administrative judge's over-arching adjudicative goal is a fair, impartial and common sense 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.

Under Directive ¶ E3.1.14, the Government must present evidence to establish controverted facts alleged in the SOR. Under Directive ¶ E3.1.15, the applicant is responsible for presenting "witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by applicant or proven by Department Counsel. . . ." The applicant has the ultimate burden of persuasion in seeking 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 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 describes the Guideline K security concern as follows: "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. . . ."

The SOR Guideline K allegations, which Applicant admitted, raise security concerns under the following Guideline K disqualifying conditions: AG ¶¶ 34(a), 34(b), 34(c), 34(e), and 35(g). AG ¶ 34(a) reads: "deliberate or negligent disclosure of classified or other protected information to unauthorized persons, including but not limited to personal or business contacts, to the media, or to persons present at seminars, meetings, or conferences." AG ¶ 34(b) reads: "collecting or storing classified or other protected information at home or in any other unauthorized location." AG ¶ 34(c) reads: "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." AG ¶ 34(e) reads: "copying classified or other protected information in a manner designed to conceal or remove classification or other documents control marking." AG ¶ 34(g) reads: "any failure to comply with rules for the protection of classified or other sensitive information."

Under Guideline K, there are three mitigating conditions. AG ¶ 35(a) reads: "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." AG ¶ 35(b) reads: "the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities." AG ¶ 35(c) reads: "the security violations were due to improper or inadequate training."

The incidents that gave rise to security concerns occurred in 2007, and they are therefore recent. Applicant's security incidents did not take place under unusual circumstances. Instead, they occurred during the normal course of his work, when he willfully carried out actions he knew to be in violation of rules for the protection of classified information. Applicant was a career military officer; he knew the rules for protecting classified information and chose to disregard them for his own convenience. While he has subsequently taken remedial security training and appears positive about discharging security responsibilities, he failed to offer a rational explanation for his former security violations or to offer credible assurances that the behavior would not happen again in the future. I conclude that none of the Guideline K mitigating conditions applies to the facts of Applicant's case.

Guideline E, 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." AG ¶15.

The SOR alleged that Applicant's failure to comply with rules and regulations pertaining to handling protected information also raised security concerns under Guideline E, Personal Conduct. Specifically, allegations of Appellant's alleged personal conduct related to allegations in SOR ¶¶ 1.a. through 1.c, which were cross-alleged under Guideline E at SOR ¶ 2.a. Additionally the SOR alleged disqualifying personal conduct when Applicant directed a contract employee to violate rules for protecting classified information and then also directed him not to tell anyone of the violation. (SOR ¶ 2.b.)

Applicant, a career military officer who had been thoroughly trained in procedures for protecting classified information, knowingly violated those procedures and directed a contract employee not to divulge one of his violations. Applicant concealed his violations for several months. He did not reveal his disqualifying conduct until the contract employee was investigated for a security breach and implicated Applicant. This conduct raises security concerns under AG ¶16(e)(1), which reads: "personal conduct, or concealment of information about one's conduct, that creates a vulnerability to exploitation, manipulation, or duress, such as (1) engaging in activities which, if known, may affect the person's personal, professional, or community standing."

Several Personal Conduct mitigating conditions might have applicability in this case. If "the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts," then AG ¶ 17(a) might apply. If "the offense is so minor, or so much time has passed, or the behavior is so infrequent, or if 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," then AG ¶ 17(c) might apply. If "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," then AG ¶ 17(d) might apply. If "the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress," then AG ¶ 17(e) might be applicable.

Applicant came forward after several months and admitted the conduct he had concealed about his security violations, but only after he was implicated by the contract employee. Accordingly, AG ¶ 17(a) has limited applicability. Applicant's security violations were not minor, and they occurred recently. They cast doubt on his reliability, trustworthiness, and judgment. I conclude that AG ¶ 17(c) does not apply.

Applicant acknowledged that he knew the rules and regulations for protecting classified information and chose nevertheless to violate them. He provided documentation showing that he had taken an independent study course in basic security matters. AG ¶ 17(d) therefore has some applicability. However, Applicant did not provide evidence to establish that he had taken positive steps to reduce his vulnerability to exploitation, manipulation, or duress that was caused by concealing his security violations. When Applicant admitted his rule-breaking conduct to his chain of

command and to his supervisor, he lessened his vulnerability to exploitation, manipulation, or duress. I conclude, therefore, that AG ¶ 17(e) has some applicability to the facts of this case.

Guideline M, Use of Information Technology Systems

AG ¶ 39 describes the Guideline M security concern as follows:

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

The SOR cross-alleges at ¶ 3.a. that the Guideline K conduct alleged at SOR ¶¶ 1.a. and 1.b. also raises security concerns under Guideline M. In 2007, Applicant improperly handled and stored classified information on his personal unclassified laptop computer, in violation of a lawful general regulation that he, as a military officer, was obligated to comply with. Additionally, even though he did not have authority to classify or declassify classified information, Applicant removed classified markings from classified photographs in order to move them from a classified computer network to an unclassified network.

Applicant's actions raise Guideline M security concerns under AG ¶¶ 40(d) and 40(f). AG ¶ 40(d) reads: "downloading, storing, or transmitting classified information on or to any unauthorized software, hardware, or information technology systems." AG ¶ 40(f) reads: "introduction, removal, or duplication of hardware, firmware, software, or media to or from any information technology system without authorization, when prohibited by rules, procedures, guidelines or regulations."

There are three conditions that could mitigate Guideline M security concerns. If "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," then AG ¶ 41(a) might apply. If "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," then AG ¶ 41(b) might apply. Finally, if "the conduct was unintentional or inadvertent and was followed by a prompt good-faith effort to correct the situation and by notification of supervisor," then AG ¶ 41(c) might apply.

Applicant's disqualifying conduct, which occurred in 2007, is recent, did not occur under unusual circumstances, and casts doubt on his reliability, trustworthiness, and

good judgment. Applicant's misuse of information technology was not minor, and it was intentional. It was not done in the interest of organizational efficiency but to serve Applicant's own purposes. Applicant did not attempt to correct the situation and notify his supervisor until he was implicated in the courier's security violation. I conclude that none of the Guideline M mitigating conditions applies to the facts of Applicant's case.

Whole-Person Concept

Under the whole-person concept, the administrative judge must evaluate an applicant's eligibility for a security clearance by considering the totality of the applicant's conduct and all relevant circumstances. The administrative judge should consider the 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. Applicant is a mature adult. His former commander and his current supervisor consider him to possess good character and to be a diligent employee. As a military officer trained in security procedures and in protecting classified information, he chose to violate security rules and regulations to serve his own purposes. As a program officer and director of a component unit, Applicant also had responsibilities to lead by example and to model good procedures for the protection of classified information. Instead, he violated security procedures by failing to sign a chain of custody document when he took possession of classified information. He then elected to work on classified information in his home, an unsecure location, and he directed a courier not to tell anyone that he had violated security rules. He concealed his security violations until he was implicated in the courier's later security violation.

I observed Applicant carefully at his security clearance hearing. Applicant was clearly concerned that his rule-breaking behavior caused damage to his career. He seemed to be less concerned about the impact his rule-breaking had on his unit and those who reported to him. While he stated that he would never again violate regulations for the protection of classified information, Applicant's assertions were not

credible. I am not persuaded that, in the future, he would put the Government's interests before his own in the protection of classified information.

Overall, the record evidence leaves me with questions and doubts about Applicant's judgment and his eligibility and suitability for a security clearance. I conclude that Applicant failed to mitigate security concerns arising under Guideline K, Guideline E, and Guideline M.

Formal Findings

Formal findings for or against Applicant on the allegations set forth in the SOR, as required by section E3.1.25 of Enclosure 3 of the Directive, are:

Paragraph 1, Guideline K:	AGAINST APPLICANT
Subparagraphs 1.a. through 1.c.:	Against Applicant
Paragraph 2, Guideline E:	AGAINST APPLICANT
Subparagraphs 2.a. and 2.b.:	Against Applicant
Paragraph 3, Guideline M:	AGAINST APPLICANT
Subparagraph 3.a. :	Against Applicant

Conclusion

In light of all of the circumstances presented by the record in this case, it is not clearly consistent with the national interest to grant Applicant eligibility for a security clearance. Eligibility for access to classified information is denied.

_____
Joan Caton Anthony
Administrative Judge