DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 11-11874
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Richard Stevens, Esq., Department Counsel
For Applicant: Drew Early, Esq.

07/18/2013

Decision

DUFFY, James F., Administrative Judge:

Applicant failed to mitigate security concerns arising under Guideline E (Personal Conduct), Guideline K (Handling Protected Information), and Guideline M (Use of Information Technology Systems). Clearance is denied.

Statement of the Case

On December 31, 2012, the Department of Defense (DOD) issued Applicant a Statement of Reasons (SOR) detailing security concerns under Guidelines E, K, and M. This action was taken under Executive Order 10865, *Safeguarding Classified Information Within Industry,* dated February 20, 1960, as amended; Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program,* dated January 2, 1992, as amended (Directive); and the adjudicative guidelines (AG) implemented on September 1, 2006.

The SOR detailed reasons why DOD could not find under the Directive that it is clearly consistent with the national interest to grant or continue Applicant's security clearance. On February 15, 2013, Applicant answered the SOR and requested a

hearing. The case was assigned to me on April 15, 2013. DOHA issued the Notice of Hearing on May 2, 2013. The hearing was held as scheduled on June 4, 2013. Department Counsel called two witnesses and offered exhibits (GE) 1 through 8. Applicant testified and offered exhibits (AE) 1 through 12. All exhibits were admitted into evidence without objection. DOHA received the transcript (Tr.) of the hearing on June 12, 2013.

Procedural Matters

At the start of the hearing, Department Counsel withdrew the Guideline E allegations in SOR ¶¶ 1.a and 1.b.

Findings of Fact

Applicant is a 52-year-old employee of a defense contractor. He began working for his current employer in March 2011. He received a bachelor's degree in 1983, earned a certificate of completion from a military war college in 2007, and completed defense acquisition courses between 2003 and 2010. He served in the U.S Army and Army Reserve for about 32 years and retired in the grade of lieutenant colonel (O-5). He is married and has four children, ages 16, 21, 23, and 26. He has held a security clearance for about 30 years.[1]

The remaining Guideline E allegation, SOR ¶ 1.c, alleged that Applicant copied in excess of 5,000 proprietary documents onto a flash drive on his last day of work at a company (hereafter referred to as "Company I"), failed to return the flash drive when initially asked, and subsequently retrieved it from his vehicle. The allegation in SOR ¶ 1.c was cross-alleged as the only allegation under Guidelines K and M. In his Answer to the SOR, Applicant admitted that he downloaded files on his last day of work at Company I, but stated that he was only attempting to copy his personal files. His admission, as explained in his Answer to the SOR, is incorporated as a finding of fact.[2]

Applicant started working at Company I in August 2009. He worked there as a senior program analyst. At the beginning of that employment, he signed a confidentiality requirements document. This document indicated that maintaining confidentiality of sensitive information was important to Company I's competitive position in the industry and ultimately to its success. It also stated in part:

> Protect this information by safeguarding it when in use, filing it properly when not in use, and discussing it only with those who have a legitimate business need to know. Employees are not to disclose (whether in one-on-one or small discussions, meetings, presentations, proposals or

[1] Tr. 13, 62; GE 1; AE 6, 7; Applicant's Answer to the SOR.

[2] Tr. 8; Applicant's Answer to the SOR.

otherwise) any material nonpublic information with respect to [Company I], its business operations, plans, financial condition, results of operations or any development plan.

You must keep confidential and not disclose to others, without prior written approval from the Vice President of [Company I], all information developed, disclosed, found or learned by you in the course of your employment with [Company I]. Everything except that which is intended for outside distribution should be considered proprietary. This information includes, but is not limited to: reports and surveys, formulae, processes, plans, drawings, diagrams, apparatus, mechanisms, tools, equipment, designs, specifications, confidential business information, budgets, financial reports, customer and supplier lists, confidential cost and pricing information, computer source codes, computer programs, manuals, concepts, techniques, methods, systems, circuits, research, development or experimental work, work in process, operations, schedules of employee compensation, personnel records, account records, and trade secrets and confidential business and technical information received from third parties that is subject to a duty to maintain such confidentiality. If you are asked to reproduce documents for someone, either inside or outside the company, and are uncertain whether those documents are confidential, you should check with your supervisor. Dissemination of proprietary information without authorization may result in disciplinary action, up to and including termination.[3]

An employee handbook and a security handbook that contained information on safeguarding proprietary information were posted on the company's website. Applicant certified that he read and understood the company's security handbook in April 2010.[4]

Applicant testified that, around February 18, 2011, his supervisor informed him that the company was running out of work for him. While continuing to work at Company I, he found another job. On March 16, 2011, he submitted a letter of resignation that indicated leaving Company I was not an easy decision for him to make. The letter stated that his resignation would be effective March 27, 2011.[5]

On Tuesday, March 22, 2011, Applicant downloaded about 5,000 files from Company I's computer system onto a flash drive. On Thursday, March 24, 2011, Applicant informed Company I's IT administrator that he was resigning and asked the IT

[3] Tr. 39, 47-48, 64-69; GE 1, 4.

[4] Tr. 21-23, 39; AE 11. The company's information technology (IT) administrator testified that he thought the employee handbook stated that proprietary information could not be taken from Company I's building without prior approval.

[5] Tr. 61; GE 5.

administrator to make a compact disc (CD) of his personal documents and email files. The IT administrator advised him to create a computer folder with his personal documents so that the administrator could easily identify and copy them.[6]

The following day, Friday, March 25, 2011, was Applicant's last day of work at Company I. On that morning, he advised the IT administrator that the folder was ready. When the IT administrator attempted to copy the folder, he noticed that it contained several thousand documents totaling almost three gigabytes of data. In the folder, he noticed files related to a company program (Program F) and other company business. He checked the computer monitoring logs and saw that Applicant had copied on Tuesday of that week over 5,000 documents, including some pertaining to Program F, to a flash drive. The IT administrator advised Applicant's supervisor of the documents that Applicant had copied. The supervisor confirmed that Applicant should not be in possession of those documents. The supervisor indicated that he would talk to Applicant and retrieve the flash drive.[7]

At a later point, Applicant told the IT administrator that the flash drive was in a box at his home, and he would return it on Monday. The IT administrator was suspicious of Applicant's statement and checked the computer logs. The logs showed that Applicant had been using that flash drive on his company's computer just 30 minutes earlier that day. The IT administrator informed the supervisor that the logs showed Applicant's earlier use of the flash drive. The supervisor told the IT administrator that he would talk to Applicant again.[8]

At approximately 10:00 a.m. that day, the company's human relations (HR) representative began conducting Applicant's out-processing and exit interview. During the out-processing interview, the HR representative asked Applicant whether he had any proprietary information, and Applicant stated that he did not think he had such information. At a later point, the out-processing interview was interrupted when Applicant's supervisor took Applicant to a nearby conference room. The supervisor advised the HR representative that Applicant was retrieving an item. The supervisor told the HR representative not to complete the out-processing until Applicant brought back the item and the supervisor gave her the "okay" to proceed.[9]

After Applicant retrieved the flash drive from his car, the supervisor and IT administrator went through the flash drive and deleted documents that the supervisor determined were proprietary in nature. The IT administrator estimated that he deleted

[6] Tr. 39-40, 70-71; GE 3, 8.

[7] Tr. 40-43, 50-51; GE 3, 8.

[8] Tr. 43-45, 71; GE 3, 8.

[9] Tr. 19-21, 24-28; GE 3, 7, 8.

80 to 90 percent of the documents on the flash drive. The supervisor later advised the HR representative that she could continue with Applicant's out-processing.[10]

At some point in the out-processing interview, Applicant also signed an Employee Termination Disclosure and Certification form. In that form, Applicant acknowledged:

> By signing this document I declare that I do not have in my possession, nor have I failed to return, any trade secrets, or confidential or proprietary information of the company including, but not limited to, any documents, manuals, computers, computer programs, software, keys, specifications, drawings, blue prints, reproductions, notes, reports, proposals, plans, customer lists, marketing materials, or other materials tools, equipment or other property belonging to [Company I].

It is unknown whether Applicant signed that document before or after he retrieved the flash drive.[11]

During the out-processing interview, Applicant also indicated that he no longer had any company badges. A later review of company records confirmed that he was issued a Common Access Card (CAC). On March 30, 2011, the HR representative called him at home and requested that he return the company's CAC. He stated that he forgot about that card and later returned it to the company that day. On March 30, 2011, Company I submitted a Joint Personnel Adjudication System (JPAS) entry that documented Applicant's copying of the files and the CAC incident. The JPAS entry stated that Applicant should not have been in possession of those files due to their proprietary nature.[12]

In his Answer to the SOR, Applicant described the events of his last day at work as follows:

> My employment with [Company I] was ending in March 2011, as [the company] had failed to secure additional work for me. I found a position with my current employer . . . I asked the [company] IT representative if there was a way to create a copy of my personnel files before I left. The IT rep instructed me to put all my personnel files in a folder, which I did, and they would provide me a copy of the files before I left.

[10] Tr. 43-45, 48-49; GE 3, 7, 8.

[11] Tr. 24-25; GE 6, 7.

[12] Tr. 22-24, 28-29, 60-61; GE 3, 7.

> As the last day progressed, the IT rep didn't show up, so I took a thumb drive I had and copied those files to it. Sometime later the IT rep showed up and gave me the disk with the same files.
>
> An hour later, my supervisor confronted me in a very aggressive manner about downloading the files. I was intimidated and frightened by him; I told him I had copied the files and didn't have the drive with me – which was technically true – as I had taken my stuff out to my car. Recovering my composure and in an effort to do the right thing, I retrieved the drive and gave it to him so he could see I had only copied the personnel files I had discussed with IT. I believe it is this event that triggered the JPAS entries.
>
> With[in] an hour, he returned the thumb drive, without comment. He has not spoken to me or attempted to contact me in any way shape or form since. Nor did he say there was any issue. I was on site for another hour out processing, nothing was ever said or conveyed that there was any problem.
>
> * * *
>
> As a point of fact, I did tell the employer that I had made a copy when the IT rep finally showed up with the disk with my files on it. It was shortly after that my supervisor got in my face, scaring me and questioning me about the files. As I stated before, at that point I did not have physical possession of the thumb drive, or I would have given it to him. It was in my car – which I retrieved shortly and gave to either him or the IT rep, it's been so long I can't remember who I gave it to.[13]

Applicant attributed the JPAS allegations to his former supervisor's retribution because Applicant obtained a job working for a competitor. He claimed the "inaccurate" JPAS reporting was an attempt to deny him employment, ruin his career, and destroy his reputation.[14]

During his Office of Personnel Management interview, Applicant reportedly stated that he only copied the files in good faith. At the hearing, he testified that he got "trigger happy" when he was identifying the personal and Reserve files that he intended to copy and "took too much." He stated that he did not know whether any of those files contained proprietary information, but thought that they might contain documents that could put Company I at a disadvantage, either directly or indirectly, if someone wanted to exploit them. He also acknowledged that these were not the type of documents that one would leave in public view, but noted he did not have any malicious intent in taking any of the files. In later questioning, Applicant agreed that, in retrospect, his earlier

[13] Applicant's Answer to the SOR. See also GE 2.

[14] GE 2; Applicant's Answer to the SOR.

statement that none of the information was proprietary in nature was not accurate. When asked why he told the IT administrator on his last day at work that the flash drive was at his home when that statement was not true, he replied, "I got scared, got stupid."[15]

The director of a program office at a major Army command commended Applicant for his invaluable support to that command. The director referred to him as "a self-starter with a can-do attitude" who "demonstrated unwavering dedication to the warfighter and all the leadership skills necessary to produce the required results." A manager at Applicant's current company stated that he has "shown himself to be trustworthy with use of computer network systems, meticulously following corporate and government policies . . . ."[16]

Applicant completed an impressive military career. During Operation Desert Storm, he served as a helicopter pilot and was awarded the Bronze Star Medal and Air Medal for his performance in combat. In his career, he also earned the Meritorious Service Medal, two Army Commendation Medals, and two Army Achievement Medals. His officer evaluation reports (OERs) reflect that he was a top performer. In the OERs, he was consistently marked in the highest performance categories, *i.e.*, "best qualified" and "outstanding performance, must promote," or in earlier versions of that form as "always exceeded requirements" and "promote ahead of contemporaries." At Company I, his supervisor rated him as "exceptional," which was the highest rating category. He has received many certificates reflecting his completion of various training requirements. Since he began working for his current employer, he completed ethics information assurance, and cyber awareness training.[17]

Policies

The President of the United States 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. *Department of the Navy v. Egan*, 484 U.S. 518, 527 (1988). The President has authorized the Secretary of Defense to grant 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. The U.S. Supreme Court has recognized the substantial discretion of the Executive Branch in regulating access to information pertaining to national security, emphasizing that "no one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988).

[15] Tr. 61, 63-69, 71; GE 2; Applicant's Answer to the SOR.

[16] AE 10, 12.

[17] Tr. 64; AE 1-11; Applicant's Answer to the SOR.

Eligibility for a security clearance is predicated upon the applicant meeting the criteria contained in the AGs. These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, these guidelines are applied in conjunction with an evaluation of the whole person. An administrative judge's adjudicative goal is a fair, impartial, and commonsense decision. An administrative judge must consider all available, reliable information about the person, past and present, favorable and unfavorable, to reach his decision.

The Government reposes a high degree of trust and confidence in persons with access to classified information. This relationship transcends normal duty hours and endures throughout off-duty hours. Decisions include, by necessity, consideration of the possible risk that 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. Clearance decisions must be "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." *See* Exec. Or. 10865 § 7. *See also* Executive Order 12968 (Aug. 2, 1995), Section 3. Thus, a clearance decision is merely an indication that the Applicant has or has not met the strict guidelines the President and the Secretary of Defense have established for issuing a clearance.

Initially, the Government must establish, by substantial evidence, conditions in the personal or professional history of the applicant that may disqualify the applicant from being eligible for access to classified information. The Government has the burden of establishing controverted facts alleged in the SOR. *See Egan*, 484 U.S. at 531. "Substantial evidence" is "more than a scintilla but less than a preponderance." *See v. Washington Metro. Area Transit Auth.*, 36 F.3d 375, 380 (4th Cir. 1994). The guidelines presume a nexus or rational connection between proven conduct under any of the criteria listed and an applicant's security suitability. *See* ISCR Case No. 95-0611 at 2 (App. Bd. May 2, 1996).

Once the Government establishes a disqualifying condition by substantial evidence, the burden shifts to the applicant to rebut, explain, extenuate, or mitigate the facts. Directive ¶ E3.1.15. An applicant "has the ultimate burden of demonstrating that it is clearly consistent with the national interest to grant or continue [his or her] security clearance." ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002). The burden of disproving a mitigating condition never shifts to the Government. *See* ISCR Case No. 02-31154 at 5 (App. Bd. Sep. 22, 2005). "[S]ecurity clearance determinations should err, if they must, on the side of denials." *Egan*, 484 U.S. at 531; *see* AG ¶ 2(b).

Analysis

Guideline K, Handling Protected Information

AG ¶ 33 sets forth the security concern for the handling of 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 unwillingness and ability to safeguard such information, and is a serious security concern.

I have considered all of the handling of protected information disqualifying conditions under AG ¶ 34 and the following are potentially applicable:

> (b) collecting or storing classified or protected information at home or in any other unauthorized location; and
>
> (g) any failure to comply with rules for the protection of classified or other sensitive information.

During his last week of work at Company I in March 2011, Applicant copied thousands of files from a company computer onto a flash drive. These files included information on at least one company program. At the hearing, Applicant conceded that the files were not the type that should be left in public view and believed they contained information that could put the company at a disadvantage if someone were to exploit them. In a JPAS entry, the company stated that Applicant should not have possessed them because of their proprietary nature.

On his last day at work, Applicant sought the assistance of the company's IT administrator to copy documents onto a CD. In looking at the documents, the IT administrator noticed they contained information on the company's business and also determined that Applicant had copied those or similar files onto a flash drive earlier in the week. A supervisor confirmed that Applicant should not be in possession of those files. Applicant was asked to turn over the flash drive. He lied about the flash drive's location by stating it was at his home and indicated he would return it the next workday. The IT administrator was able to determine that the Applicant had lied about its location through computer logs that showed Applicant had been using the flash drive at work earlier that morning. When confronted about the information in the computer logs, Applicant retrieved the flash drive from his car, turned it over his supervisor, and sensitive information was deleted from it.

Applicant stated that he lied about the location of the flash drive because he "got scared, got stupid." This lie is circumstantial evidence that he knew what he was doing was wrong. In his Answer to the SOR, Applicant also stated, "I did tell the employer that I had made a copy [of the files] when the IT rep finally showed up with the disk with my files on it." The IT administrator's testimony and written statement, however, contradict Applicant's statement about telling the IT administrator that he made a copy of the files. The IT administrator determined that Applicant had made a copy of the files by reviewing the computer logs.

Substantial record evidence exists to establish that Applicant knowingly copied and intended to take protected information from Company I without authorization. In

particular, he know that he was not allowed to copy such protected information onto that flash drive for his personal retention as he was leaving that company's employment. He also failed to safeguard the company's protected information by placing the flash drive in his car. The above disqualifying condition applies.

I have considered all of the handling of protected information mitigating conditions under AG ¶ 35 and the following are potentially applicable:

> (a) so much time has elapsed since the behavior, or it happened so infrequently or under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment; and
>
> (b) the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities.

No information was presented to show that Applicant disclosed protected information to an unauthorized individual. Since obtaining his current job, he has completed ethics and information assurance training.

In his Answer to the SOR, Applicant claimed that he was attempting to copy only personal files, but his reaction when confronted by his supervisor showed that he knew he should not have copied those files. In his Answer to the SOR, he also stated that he initially told his supervisor that he did not have the flash drive with him, but later regained his composure and gave the supervisor the flash drive. The record evidence, however, is more disturbing and showed that he only retrieved the flash drive after being confronted with information from computer logs that revealed he had been using the flash drive earlier in the day. Insufficient evidence has been presented to show that Applicant has accepted responsibility for attempting to take protected information from the company without authorization. While this incident happened a little over two years ago, insufficient time has passed to conclude that Applicant has reformed and rehabilitated himself. This incident continues to cast doubt on Applicant's reliability, trustworthiness, and good judgment. AG ¶¶ 35(a) and 35(b) do not 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. The following is potentially applicable:

> (f) 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.

The discussion of the facts under Guideline K applies equally here and is incorporated under this guideline. AG ¶ 40(f) applies.

I have considered all of the mitigating conditions under AG ¶ 41 and the following are potentially applicable:

> (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.

For the reasons discussed under Guideline K, none of the Guideline M mitigating conditions apply in this case.

Guideline E, Personal Conduct

The security concern for personal conduct is set out in AG ¶ 15, as follows:

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

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

> (c) credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any other single guideline, but which, when considered as a whole, supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the person may not properly safeguard protected information;
>
> (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 evidence 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; (4) evidence of significant misuse of Government or other employer's time or resources; and
>
> (e) 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 . . . .

The discussion of the facts under Guideline K applies equally here and is incorporated under this guideline. Because Applicant's copying of the protected information was explicitly covered under Guidelines K and M, AG ¶ 16(d) does not apply. However, since such copying could affect Applicant's personal, professional, or community standing, AG ¶ 16(e) applies to that conduct.

Applicant's failure to turn over the flash drive when initially asked calls into question his reliability, trustworthiness, and good judgment. AG ¶ 16(c) applies to that failure.

AG ¶ 17 lists three personal conduct mitigating conditions that 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; and
>
> (e) the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress.

For the reasons discussed under Guideline K, none of the Guideline E mitigating conditions apply.

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 relevant facts and circumstances surrounding this case. I have incorporated my comments under Guidelines E, 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 has an impressive military record. He served in the Army and Army Reserve for 32 years. He held a security clearance for most of that time. He was awarded a Bronze Star and Air Medal during Operation Desert Storm. He is highly thought of in his current job. Nevertheless, his copying of protected information from Company I's computers on his last week of work there is troubling. When confronted by his supervisor at Company I, he lied about the location of the flash drive. He has not

accepted responsibility for his inappropriate conduct. Instead, he claimed that he only intended to copy personal files and that he had no malicious intent. I did not find those claims credible.

Overall, the record evidence leaves me with questions and doubts about Applicant's suitability for a security clearance. Therefore, I conclude Applicant has not mitigated the security concerns arising under Guidelines E, K, and M.

Formal Findings

Formal findings on the allegations set forth in the SOR, as required by Section E3.1.25 of Enclosure 3 of the Directive, are:

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

Decision

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

_____
James F. Duffy
Administrative Judge