DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 14-02798
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Julie R. Mendez, Esquire, Department Counsel
For Applicant: Christopher Graham, Esquire

10/16/2015

Decision

LYNCH, Noreen A., Administrative Judge:

After reviewing of the pleadings, exhibits, and testimony, Applicant presented sufficient information to mitigate the Government's security concerns under Guideline M and Guideline E. Applicant's eligibility for access to classified information is granted.

Applicant signed an Electronic Questionnaire for Investigations Processing (e-QIP) version of a security clearance application (SF-86) on February 5, 2013. The Department of Defense (DOD) issued Applicant a Statement of Reasons (SOR), dated August 21, 2014, alleging security concerns under 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 For Determining Eligibility for Access to Classified Information* (AG) implemented on September 1, 2006.

Applicant answered the SOR in writing on September 16, 2014, and requested a hearing before an administrative judge. DOD issued a notice of hearing on July 21, 2015, and I convened the hearing as scheduled on August 21, 2015. The Government submitted three exhibits marked as GE 1 through 3, which were admitted into evidence without objection. Applicant testified and submitted three exhibits (AX A through C). DOHA received the transcript of the hearing (Tr.) on August 31, 2015.

Findings of Fact

In his Answer to the SOR, Applicant denied the factual allegations under both Guideline M and Guideline E with explanations.[1] After reviewing the entire record, I make the following findings of fact.

Applicant is 41 years old. He received his undergraduate degree in accounting, and earned a graduate degree in finance. Applicant is married and has two children. He served in the Army National Guard from 1998 until 2007, receiving an honorable discharge. He has held a security clearance since 1998. He has been with his current employer since September 2013. (Tr. 55) He serves as a financial management analyst.

In mid-2012, Applicant applied for positions through USAJobs.gov while he was still employed. The new positions required a top secret (TS) clearance. He interviewed for a position with another government contractor. He was offered a job in approximately January 2013. (Tr. 25) Applicant provided an email that verified the tentative offer. (Attachment to Answer to SOR)

Applicant's employer learned about the potential employment. (Tr. 25) Applicant's boss met with him a day or so later and told him that "he was being fired." (Tr. 27) Applicant stated that the reason for the termination was accepting another position. (Tr. 27) In reality, Applicant received a tentative offer letter, and claimed he had not accepted the position due to the necessary security investigation, which was pending. He confided that information to his supervisor. Applicant provided an email that noted the offer was tentative, and advising him to wait for a firm offer and firm salary. Also, at the time, due to possible freezes of jobs, he was not sure that the position would be filled.

Applicant received a letter from his former employer, dated March 8, 2013, stating that the company believed it was best for Applicant and the company to part ways. Two reasons were noted in the letter. The employer noted that Applicant had accepted a position with another company and that plans had been made to reduce the number of team leads on the contract. March 8, 2013 was Applicant's last day. (GX 2) Just a few days before this incident, Applicant was awarded a cash bonus for his performance at the job. Now he found himself unemployed.

At the time of his dismissal, Applicant had a company laptop in his possession. He and his wife were attending a weekend wedding out-of-town and he packed the

[1]At the start of the hearing, Department Counsel withdrew allegations 2.e and 2. f.

laptop with luggage that his wife took with her. He was to join her at the wedding and he stated that they were then taking an extended vacation. (Tr. 27) He changed his day of departure so that he could attend company training. However, after the training, he was told that he was being terminated.

The day of the dismissal, Applicant told the company that he had company supplies in separate places. The first place was at the client site, and the second place was at home. (Answer to SOR) Applicant stated in his answer that he did not want to tell the company that the laptop was out-of-state with his wife. (Answer to SOR) At that point he was concerned about promptly returning it.

On March 14, 2013, Applicant received a letter from legal counsel for his former employer. The letter noted that they monitored Applicant's laptop and knew when it was opened and that Applicant copied files to a thumb-drive. The letter further explained that the company knew that Applicant updated his resume. The letter accused Applicant of lying to the company by not telling them that the laptop was with his wife on a trip. (GX2) When Applicant returned the allegation was that the thumb-drive was blank.

Applicant and his wife returned from the wedding, and Applicant started to clean the laptop by removing personal files from it. (Tr. 31) He denied that he copied or erased Government files. He testified credibly that he attempted to copy over personal files which included his resume, bank statements, and pictures saved on the laptop. (Tr. 31) Applicant explained that there was no Government information on the laptop as required by non-disclosure agreements and other agreements that he signed with the company. (Tr. 31)

At the hearing, Applicant again denied the allegation concerning copying government files to a thumb drive. He maintained that he unsuccessfully attempted to cover over personal files which included his resume. He explained that the company laptop had nothing on it that was proprietary Government information. The company had no validation that Applicant had copied any Government files to a thumb drive.

When Applicant was interviewed in March 2013 by the security investigator, he told him the reason that he was no longer employed with his former employer. The report used the word "laid off", but it continues to state that Applicant showed him the termination letter. There is no evidence that Applicant lied to the investigator. (GX 3)

At the hearing, when questioned about the whereabouts of the laptop, Applicant stated that he told the employers that the laptop was with his wife. This is inconsistent with his statement in his answer to the SOR. He also testified that since he had just been terminated on the spot, that he was shaken at the sudden dismissal, and did not make an attempt to call his wife to get the laptop sent back immediately. (Tr. 30).

Applicant testified that he believes his dismissal and the allegations against him were the result of Applicant's statement that he would file a complaint with the Defense Contracting Agency. (Tr. 33) He wanted to file a complaint because he believed this

was unusual in that normally a contractor had to give the Government agency 30 days notice that a particular contractor was being removed from a project. (Tr. 33)

Applicant was adamant that he was authorized to have the company laptop and he admits to having a thumb drive. However, he was not authorized to do any Government work on that laptop. He made an attempt to retrieve his resume but he could not do so. He used the laptop for business correspondence, and some reports. There were no Government files on it and when he returned the thumb drive it was empty. (Tr. 62) He used a Government laptop at the contracting site for such information. (Tr. 63)

Applicant submitted three letters of recommendation, which state that he is a dedicated role model for any company. His former colleague has known him for a number of years and worked closely with him on government projects. Applicant is described as honest and trustworthy. The colleague saw the termination letter and was shocked based on Applicant's track record. (AX C)

A subordinate of Applicant's wrote that Applicant was his manager and that they worked closely together on a number of projects. He stated that Applicant was a leader and showed integrity, good judgment and dedication. He noted that Applicant has been a mentor to him for years. (AX 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.

Under Directive ¶ E3.1.14, the Government must present evidence to establish controverted facts alleged in the SOR. Under Directive ¶ E3.1.15, an applicant is responsible for presenting "witnesses and other evidence to rebut, explain, extenuate,

or mitigate facts admitted by applicant or proven by Department Counsel. . . .” An applicant has the ultimate burden of persuasion for obtaining a favorable security decision.

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

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

Analysis

Guideline 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 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.

AG ¶ 40 describes the disqualifying conditions that could raise security concerns. I have considered all the conditions, and the following: (e) unauthorized use of a government or other information technology system; (f) introduction, removal, or duplication of hardware, firmware, software, or media to or from any information technology system without authorization, when prohibited by rules, procedure, guidelines or regulations; and (g) negligence or lax security habits in handling information technology that persist despite counseling by management.

Applicant denied copying Government files to a thumb drive with his company laptop. He had authority to have the laptop in his possession. The Government did not establish that Applicant copied any Government files after being terminated from his employment. A letter from the company’s law firm, dated March 14, 2013, summarizes

policies and procedures related to the use of protecting classified information. However, not only is there no signed agreement by Applicant, there is no validation of the "copied government files." The letter cites to federal and state laws, but does not state how the computer was monitored and how the company knew that Government files were copied. The thumb drive was returned to the company. It was blank because the attempt to copy or update his personal resume was not successful. The Government has not established a *prima facie* case under Guideline M.

Guideline E: Personal Conduct

AG ¶ 15 expresses the security concern pertaining to personal conduct:

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

AG ¶ 16 describes the disqualifying conditions that could raise security concerns. I have considered all the conditions, and especially the following:

> (a) deliberate omission, concealment, or falsification of relevant facts from any personnel security questionnaire, personal history statement, or similar form used to conduct investigations, determine employment qualifications, award benefits or status, determine security clearance eligibility or trustworthiness, or award fiduciary responsibilities;
>
> (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 information supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the person may not properly safeguard protected information. This includes but is not limited to consideration of:
>
> > (1) untrustworthy or unreliable behavior to include breach of client confidentiality, release of proprietary information,

> unauthorized release of sensitive corporate or other government protected information:
>
> (2) disruptive, violent, or other inappropriate behavior in the workplace;
>
> (3) a pattern of dishonesty or rule violations; and,
>
> (4) evidence of significant misuse of Government or other employer's time or resources; and
>
> (f) violation of a written or recorded commitment made by the individual to the employee as a condition of employment.

Applicant did not lie to his company about having a tentative offer of employment. He also did not lie to the investigator about his termination because he showed him the termination letter. The Government has not established that Applicant copied any Government files onto a thumb drive after his was terminated. His behavior did not violate any policies or procedures. There is no information that was unreliable or that he had a pattern of dishonesty or rule violations. The Government did not establish a significant misuse of Government time or other time or resources. Finally, there was no information in the record that established that he violated a commitment to his employer.

The following AG ¶ 17 mitigating security concerns apply:

> (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.
>
> The inconsistent statement about when or whether he told the company about the location of the laptop, given the record as a whole, surrounding his sudden termination does not negate mitigation security concerns under Guideline E. Personal conduct has been mitigated.

Whole-Person Concept

Under the whole-person concept, the administrative judge must evaluate an applicant's eligibility for a security clearance by considering the totality of an applicant's conduct and all relevant circumstances. The administrative judge should consider the nine adjudicative process factors listed at AG ¶ 2(a):

> (1) the nature, extent, and seriousness of the conduct; (2) the circumstances surrounding the conduct, to include knowledgeable participation; (3) the frequency and recency of the conduct; (4) the individual's age and maturity at the time of the conduct; (5) the extent to

which participation is voluntary; (6) the presence or absence of rehabilitation and other permanent behavioral changes; (7) the motivation for the conduct; (8) the potential for pressure, coercion, exploitation, or duress; and (9) the likelihood of continuation or recurrence.

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

In reaching a conclusion, I considered the potentially disqualifying and mitigating conditions in light of all the facts and circumstances surrounding this case. Applicant served honorably in the U.S. military. He is married and has children. He has held a security clearance for many years without incident. He has letters of recommendation from several persons. He is an educated man who values his work.

Applicant was terminated by his company because he sought other employment. He received a tentative offer of employment and told his employer. He was terminated without any notice and had to return his laptop and other items. He was credible in his explanations that he told the Government investigator that he was terminated. The government did not establish that Applicant copied any Government files or that he lied to anyone. The fact that there is an inconsistent statement about the location of the laptop at the time of the sudden termination does not rise to a credibility concern in light of all factors considered.

For all these reasons, I conclude the Government has not met its burden to show that Applicant violated Guideline M or Guideline E.

Formal Findings

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

Paragraph 1, Guideline M:	FOR APPLICANT
Subparagraph 1.a:	For Applicant
Subparagraph 1.b:	For Applicant
Paragraph 2, Guideline E:	FOR APPLICANT

Subparagraphs 2.a-d	For Applicant
Subparagraphs 2.e, 2.f:	WITHDRAWN

Conclusion

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

Noreen A. Lynch
Administrative Judge