DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 17-01856
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Carroll Connelley, Esq., Department Counsel
For Applicant: Jeffery D. Billet, Esq.

10/10/2018

Decision

BENSON, Pamela C., Administrative Judge:

Applicant failed to mitigate the security concerns under Guideline E (Personal Conduct) and Guideline M (Use of Information Technology). National security eligibility for access to classified information is denied.

Statement of the Case

On May 28, 2015, Applicant submitted a security clearance application (SCA). On September 22, 2017, the Department of Defense Consolidated Adjudications Facility (DOD CAF) issued Applicant a Statement of Reasons (SOR), detailing security concerns under Guideline E (Personal Conduct), and Guideline M (Use of Information Technology). (Items 1 and 3) The action was taken under Executive Order (EO) 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; DOD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the Adjudicative Guidelines (AG) effective within the DOD on June 8, 2017.

Applicant answered the SOR on October 21, 2017, and he provided documents with his response. Applicant obtained counsel and requested a hearing before an

administrative judge. He denied SOR allegations ¶¶ 1.a and 2.a. He admitted in part, and denied in part, SOR allegations ¶¶ 1.b and 1.c. On May 2, 2018, the case was assigned to me. On May 29, 2018, the Defense Office of Hearings and Appeals (DOHA) issued a notice of Hearing, setting the hearing for June 13, 2018.

During the hearing, Department Counsel offered Government Exhibit (GE) 1 through 4 into evidence. Applicant's counsel objected to GE 3 and GE 4, which I admitted into evidence over counsel's objection. Applicant's counsel offered Applicant Exhibit (AE) A through O, which I entered into evidence without objection. Applicant also called his daughter to testify on his behalf. I held the record open until July 13, 2018, in the event either party wanted to submit additional documentation. No additional information was received by either party. DOHA received the hearing transcript (Tr.) on June 21, 2018, and the record was closed on July 13, 2018.

Evidentiary Ruling

Applicant's counsel objected to the admissibility to GE 3, which appears to be a Memorandum for the Record (MFR) dated August 2017, providing information about Applicant's investigation, with attached invoices submitted by Applicant, and the investigative findings. It also reports an admission by Applicant that he fabricated the invoices. The basis for counsel's objection was on multiple grounds, to include it does not fit any exception to the hearsay rule, it's inherently unreliable, the attached exhibits are illegible, and the document is an incomplete summary. In addition, counsel objected to GE 4, which is a JPAS entry. Applicant's Counsel acknowledged that a JPAS entry is an official record created in the regular course of DOD business, but his objection to this particular JPAS entry is that it is unreliable, and because the JPAS entry is hearsay. The JPAS entry with Applicant's statement at his hearing is cumulative. I gave Applicant's hearing statement greater weight than the JPAS entry.

The MFR is an investigative report summary from Applicant's former employer, with attached fraudulent receipts that Applicant provided for reimbursement, all of which are relevant and material evidence. Applicant's admissions are of a party opponent and according to Federal Rule of Evidence 801(d)(2), they are not hearsay. Investigative reports constitute an official record within the meaning of Directive ¶ E3.1.20, and as such they are admissible without an authenticating witness. *See* ISCR Case No. 08-08085 at 4 n.3 (App. Bd. Apr. 21, 2010). The JPAS entry is an official record conducted in the regular course of business by the DOD. It substantiates information in the MFR, and the JPAS entry was created at or near the time of the security incident. In addition, JPAS is the system used by DOD to determine, in part, the security eligibility information for all DOD civilian and military personnel and DOD contractors. The National Industrial Security Program Operating Manual (NISPOM) makes it a requirement for all DOD contractors to report security incidents in JPAS, which Applicant's former employer did in this instance, as required. The JPAS entry has information that corroborates the MFR, and it also reports Applicant's admission. Thus, I overruled counsel's objection to both exhibits, admitted both GE 3 and GE 4 into

evidence, and I have accorded the facts therein the appropriate weight given the record as a whole.

Findings of Fact

Having thoroughly considered the evidence in the record, I make the following findings of fact: Applicant is 48 years old. He earned a bachelor's degree in 2007, and master's degrees in 2012 and 2017. He is currently pursuing a Ph.D. in computer science with a focus in cyber security. Applicant was married in 1993 and divorced in 1999. He remarried in 1999. He has two adult children, ages 26 and 23. He has three adult stepdaughters, ages 47, 40, and 38. (Tr. 36-37; GE 1)

Applicant enlisted in the Army National Guard in December 1993. He received a general discharge under honorable conditions in January 1996 due to being absent without leave. Applicant was previously employed by a DOD contractor from April 2009 until February 2015. He submitted his resignation to this employer in February 2015, and he was unemployed the following one-to-two months. Applicant started employment with another DOD contractor in April 2015. He is an electrical engineering manager and supervises approximately 19 employees. Applicant currently possesses a Top Secret DOD security clearance. (Tr. 32-33, 38-40; GE 1)

SOR allegation ¶ 1.a alleges that Applicant resigned from his employment in February 2015, in lieu of termination by his former employer, due to falsifying financial documents he submitted for reimbursement during temporary duty assignments. Applicant admitted that he submitted his resignation in February 2015, but denied that he did so in lieu of termination. Department Counsel submitted a JPAS Incident History document (GE 4) dated March 5, 2015, which states:

> Between October 2014 and February 2015, …Special Investigations conducted an investigation on this employee. In November and December 2014, the employee was interviewed by … investigators. During the interview, the employee admitted that he had created and fabricated monthly invoices throughout his Temporary Duty (TDY) assignment period. Subsequent investigative activities substantiated his admission. On 12 Feb 2015, a Disciplinary Review Board (DRB) was held and it was determined that the employee would be allowed to Resigned (sic) in-lieu-of Termination. Additionally, he will be coded in the … Hiring database as "Not eligible for rehire."

Applicant testified that he did not falsify his reimbursable expenses during his TDY assignment, which began in the fall of 2013. He submitted financial documentation through an expense reporting system via computer, to include invoices for services and maintenance for his permanent residence, as well as expenses related to his rental house and other expenditures while TDY. Applicant submitted invoices for pool service and lawn service at his permanent residence, and he stated that no one, to include his supervisor, ever questioned the validity of these reported expenses. (Tr. 43-49; AE D)

Applicant testified that he had a Hispanic man who took care of his lawn, and he had another Hispanic man who maintained the pool at his home. Applicant and his spouse always paid these workers in cash. These workers spoke little English and were not sophisticated businessmen who provided customer receipts. Applicant created his own invoices for these paid services which he submitted to his former employer for reimbursement. Applicant made the invoices on his computer by using a template. When Applicant was asked at the hearing why the submitted invoices looked like authentic business invoices, Applicant explained he did this only to assist him with his record keeping. The invoices were never intended to defraud the company. (Tr. 50-54; 112-117; AE E, F)

Applicant was also questioned why the invoices were numbered in a random way, and why he had some invoices showing "N&R Landscaping," but on the bottom of the same invoice, in small print: "Make all checks to CNA Landscaping." Applicant stated that the numbering of the invoices was most likely "auto-generated," but he was not completely certain. His explanation for the interchangeable CNA and N&R Landscaping on the same invoice was that he had used the invoice for CNA Landscaping during a previous TDY assignment that was saved in his computer. Applicant stated he never paid by check, he paid all services in cash. The TDY rules allow $300 per month for lawn and pool maintenance expenses, and Applicant submitted invoices for these services in the amount of about $270 every month. During his background Subject Interview, Applicant told the investigator that he had a handwritten receipt from a teenager in the neighborhood who mowed his lawn. Applicant admitted during cross examination that the teenager's services (rather than his previous reference to an Hispanic man) were invoiced by Applicant as N&R Landscaping. (Tr. 114-116, 124 138-139)

Applicant's former employer first became suspicious that Applicant had fabricated a moving expense of about $2,000, after a finance analyst questioned Applicant's TDY status in late October 2014. Applicant's former employer initiated an investigation, which concluded that Applicant did, in fact, submit fraudulent financial records, to include records for pool services, moving services, furniture lease expenses, lodging expenses, for a combined total of $11,893.75. In addition, the investigation found suspected fraudulent expenses for lawn services, rental car gas/oil change expense, and tools and small equipment charges, which totaled $2,217.51. (GE 3)

Applicant testified that when his initial TDY assignment was completed in late 2014, he saw that there were funds available for a move from his TDY location back to his residence. When his new TDY status started shortly thereafter, there were also funds available to move from his residence back to the same TDY location. The maximum limit for the move was 2,000 pounds, and Applicant claimed 2,000 pounds of items moved on both occasions. Applicant hired his daughter to do both moves for him. Applicant estimated both moves at the 2,000 pound limit, but he also admitted that he never weighed the moving truck on either occasion. (Tr. 55-63, 117-122)

Applicant claimed that his daughter had just started her own moving company with a Las Vegas address. At that time his daughter did not actually live in Las Vegas, but it was her intention to eventually move there. Applicant did not keep the receipts for the moving boxes and other supplies he purchased for the move, nor did he keep receipts for the gas expense. His daughter did not know how to bill the move, so together they accessed a website and created the invoices, which were then submitted for reimbursement. The invoice did not cite his daughter's name, but a logistics company with a logo. The listed address for the moving company's invoice was obtained after they drove by a property that his daughter considered as a possible location for her new business. Applicant admitted that his daughter never moved into that property, and her moving business has not moved any other clients. The logo on the invoice is not a registered logo used by the company. The moving invoice dated September 29, 2014, (from TDY location to his residence) totaled $2,209.04, and the moving invoice dated October 8, 2014, (from his residence back to TDY location) totaled $2,294.04. Applicant claimed that he had some furniture from his brother-in-law that needed to be returned from his TDY location. Applicant brought his own personal items on the move back, just a little over a week later, to his TDY location. Applicant testified that he spoke about the move details with his supervisor, and she did not have a problem with it. No substantiating information about this conversation was provided by his former supervisor at the hearing. Applicant stated he paid approximately $4,000 in cash to his daughter for her moving services. He did not provide a cancelled check showing a $4,000 payment to her. (Tr. 55-63; 117-120, AE G; GE 3)

Applicant rented a home at his TDY location, and he also needed to rent furniture for the home. Applicant submitted a contract for the rent-to-own furniture at the hearing. (AE H) He stated that his former employer approved the contract. Applicant did not submit any itemized expense report or statements for the weekly rental transactions, despite that the expenses were billed to his corporate credit card. Applicant created another invoice showing that the monthly cost of the rent-to-own furniture was $430, which he submitted for reimbursement. Applicant stated; "So, I just created a document that would allow them (former employer) to see what exactly was getting paid for…those are the documents I made to verify those expenses." (Tr. 64-67; AE H, I)

I questioned Applicant about the contract for the rent-to-own furniture, which showed on the contract the weekly rental rate was $76.16. (AE H) When I calculated four-and-a-half weeks by this amount, it showed that at most, he should only have a monthly cost of about $342.72 to rent furniture. I asked why Applicant submitted invoices for a monthly cost of $430, when this could not possibly be the correct amount. (AE I; GE 3) Applicant admitted he mistakenly invoiced the wrong amount, and he had to repay back the difference to his former employer. Applicant also stated that his former employer estimated approximately $10,000 of expenses that were disapproved for legitimate reimbursement. Applicant chose to reimburse his former employer the $10,000 rather than pursue legal action to dispute it. He also paid this money because he did not want to receive a bad credit rating. (Tr. 96-99, 139-141)

Applicant's former employer provided information about the investigation in GE 3, dated August 31, 2017. It disclosed that: Applicant "was interviewed and admitted he fabricated numerous invoices since his TDY began in 2013, to include the $2,000 moving receipt." Applicant "only admitted to fabricating these invoices after three hours of questioning and only after the investigator left the interview room to contact several of the business people." Applicant "would not acknowledge if services were actually rendered by these businesses nor was he able to prove otherwise." Applicant's admission during the investigation is also substantiated by the JPAS Incident History record, which was reported on March 5, 2015. (GE 4)

At the hearing, Applicant denied ever using the word "fabricate" during his investigation. He testified that he told the investigators that he "created" the receipts due to the nature of the businesses that he was using, and he just wanted to be reimbursed the money he paid to these businesses. Applicant did not sign or write his own statement. The term "fabricate" can be fairly interpreted to be consistent with Applicant's statement at his hearing that he generated, manufactured, or fabricated the invoices he submitted on his computer. Applicant also denied that he failed to acknowledge whether the services were rendered during the investigation. (Tr. 84-90, 99; AE K, L)

Applicant was questioned about the date of his employment resignation that was e-mailed to his former employer, on February 12, 2015. (AE M) This was also the same date the Disciplinary Review Board determined that the employee would be allowed to resign in-lieu-of termination. (GE 4) Applicant said this was a coincidence because he did not know the Disciplinary Review Board was going to offer him the option of resignation in-lieu-of termination. Applicant reiterated that he resigned from his former place of employment due to receiving a job offer from another DOD contractor, and not for any other reason. (Tr. 129,137)

SOR allegation ¶ 1.b alleges in February 2015, without company permission, Applicant downloaded approximately 3,000 electronic files from his former employer's computer system. Similarly, SOR allegation ¶ 1.c alleges in February 2015, without company permission, Applicant downloaded approximately 3076 proprietary information files from his former employer's computer system. Applicant testified he had already submitted his employment resignation, and he received a message that a security manager was coming to his TDY location the next day to collect all of the company owned items. Applicant only had about 24 hours to save some of his personal files on the company computer. Due to the limited time constraint, Applicant decided to download all of the files from his former employer's computer, to include some files that contained proprietary information. Applicant admitted that he had received training on the protection of classified and proprietary information. Applicant admitted copying the files in haste, which he now knows was a mistake. (Tr. 100-105, 133)

The security manager apparently knew beforehand that Applicant had copied the computer files. When the security manager arrived, he asked Applicant to also hand over the external hard drives. Applicant did not understand why he was asking him for the hard drives. The security manager told Applicant that he had downloaded files from

the company computer system. Applicant confirmed he had and he gave the external hard drives to the security manager. Applicant denied he copied his former employer's proprietary information for any nefarious purposes, even though he was starting new employment with a competitor of his former employer. (Tr. 105-110)

Applicant denied SOR ¶ 2.a under Guideline M (Misuse of Information Technology), which cross-referenced the information alleged in SOR ¶¶ 1.b and 1.c. This information was addressed above, and no further comment is required.

Policies

When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the AG. In addition to brief introductory explanations for each guideline, the AG 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 national security eligibility will be resolved in favor of the 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. 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 as to 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 that an applicant may deliberately or inadvertently fail to 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 EO 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 E: Personal Conduct

AG ¶ 15 expresses the security concern for 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 or sensitive information. Of special interest is any failure to provide truthful and candid answers during national security investigative or adjudicative processes. …

The following disqualifying conditions under AG ¶ 16 are potentially applicable:

> AG ¶ 16(b) applies to these facts and circumstances: deliberately providing false or misleading information; or concealing or omitting information, concerning relevant facts to an employer, investigator, security official,…in making a recommendation relevant to a national security eligibility determination, … and;
>
> AG ¶ 16(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 individual may not properly safeguard classified or sensitive information. This includes, but is not limited to:
>
> > (3) a pattern of dishonesty or rule violations; and
> >
> > (4) evidence of significant misuse of Government or other employer's time or resources.

The SOR alleges that Applicant falsified financial documents he submitted to his former employer for reimbursement. Applicant's former employer initiated an

independent investigation which concluded that Applicant did, in fact, submit fraudulent financial records, to include invoices for pool services, moving services, furniture lease, and lodging expenses, for a combined total of $11,893.75. In addition, the investigation found suspected fraudulent expenses submitted for lawn services, rental car gas/oil change, and purchases for tools and small equipment. The suspected fraudulent expenses totaled $2,217.51. Applicant also downloaded thousands of electronic files, to include proprietary information files, from his former employer's computer system after he submitted his employment resignation. The above disqualifying conditions apply.

The guideline also includes conditions that could mitigate security concerns arising from personal conduct. The following mitigating conditions under AG ¶ 17 are potentially applicable:

> (a) the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts;
>
> (c) the offense is so minor or so much time has passed, or the behavior is so infrequent, or 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; and
>
> (d) the individual acknowledged the behavior and obtained counseling to change the behavior or taken other positive steps to alleviate the stressors, circumstances, or factors that contributed to untrustworthy, unreliable, or other inappropriate behavior, and such behavior is unlikely to recur.

None of the mitigating conditions apply. Applicant's exhibits H and I corroborate the allegation that he submitted false invoices. Applicant's costs for furniture rental was approximately $343 per month, but he submitted an invoice for $430 per month to his former employer for reimbursement. I find Applicant's submission of fraudulent invoices demonstrates conduct involving questionable judgment and an unwillingness to comply with rules and regulations. He claimed the invoices he created matched his actual expenses. He did not prove his invoices matched his actual expenses. His inability to be completely honest about the circumstances of his misconduct over a long period of time does cast doubt on his reliability, trustworthiness and good judgment. Applicant's failure to acknowledge responsibility for his actions shows there is a strong possibility his fraudulent behavior may recur. Applicant is highly educated and an IT professional. There is no reasonable excuse for downloading thousands of files from his former employer's computer system, to include his former employer's proprietary information, without prior authorization.

Guideline M, Use of Information Technology

The security concern relating to the use of information technology is set out in AG ¶ 39:

> Failure to comply 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 includes any computer-based, mobile, or wireless device used to create, store, access, process, manipulate, protect, or move information. This includes any component, whether integrated into a larger system or not, such as hardware, software, or firmware, used to enable or facilitate these operations.
>
> The following disqualifying conditions under AG ¶ 40 are potentially applicable:
>
> (d) downloading, storing, or transmitting classified, sensitive, proprietary, or other protected information on or to any unauthorized information technology system; and
>
> (e) unauthorized use of any information technology system.

The SOR alleges that Applicant downloaded thousands of electronic files, to include proprietary information files, from his former employer's computer system, without authorization. AG ¶¶ 40(d) and (e) apply.

> The following mitigating conditions under AG ¶ 41 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;
>
> (c) the conduct was unintentional or inadvertent and was followed by a prompt, good-faith effort to correct the situation and by notification to appropriate personnel; and
>
> (d) the misuse was due to improper or inadequate training or unclear instructions.

None of the mitigating conditions listed in AG ¶ 41 are applicable for the same reasons discussed in the personal conduct section, *supra*.

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 circumstances. The administrative judge should consider the nine adjudicative process factors listed at AG ¶ 2(d):

(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. This SOR highlights serious offenses that provides insight to a person's character and integrity. Applicant is not remorseful for his misconduct. His explanations are self-serving and insincere. I conclude that Applicant has not mitigated security concerns raised by his personal conduct, and use of information technology. Accordingly, Applicant has not carried his burden of showing that it is clearly consistent with the national interest to continue his eligibility for access to classified information.

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 E:	AGAINST APPLICANT
Subparagraphs 1.a-1.c:	Against Applicant
Paragraph 2, Guideline M:	AGAINST APPLICANT
Subparagraph 2.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 security to grant Applicant's eligibility for a security clearance. Eligibility for access to classified information is denied.

Pamela C. Benson
Administrative Judge