DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 19-02446
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Bryan J. Olmos, Esq., Department Counsel
For Applicant: Ernst "Mitch" Martzen, Esq., and Paul Jones, Esq.

01/12/2021

_____

Decision

_____

Gregg A. Cervi, Administrative Judge

This case involves security concerns raised under Guidelines M (Use of Information Technology) and E (Personal Conduct). Eligibility for access to classified information is denied.

Statement of the Case

Applicant submitted a security clearance application (SCA) on September 22, 2017. On October 4, 2019, the Department of Defense Consolidated Adjudications Facility (DOD CAF) sent him a Statement of Reasons (SOR) alleging security concerns under Guidelines M and E. The DOD CAF acted under Executive Order (Exec. Or.) 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 *National Security Adjudicative Guidelines for Determining Eligibility for Access to Classified Information or Eligibility to Hold a Sensitive Position* (AGs), applicable to all adjudicative decisions issued on or after June 8, 2017.

Applicant responded to the SOR on October 31, 2019, and requested a hearing before an administrative judge. The case was assigned to me on January 8, 2020. The Defense Office of Hearings and Appeals issued a notice of hearing on February 10, 2020, for a hearing to be convened on March 24, 2020. However, the hearing was canceled due to COVID-19-related cessation of travel and courtroom availability.

On July 23, 2020, Applicant's counsel submitted a motion to withdraw Applicant's request for a hearing due to delays caused by the COVID-19 pandemic, and requested a decision based on the administrative record. He submitted his intended exhibits with his motion. On July 27, 2020, Department Counsel opposed the motion pursuant to DOD Directive 5220.6, Additional Procedural Guidance §§ E3.1.7 and E3.1.8, and requested a hearing.

On July 29, 2020, I denied Applicant's motion and discussed the options of holding a hearing in a DOHA hearing room, the possibility of future travel to Applicant's location, or a video teleconference if one could be arranged. A video teleconference was arranged and a Notice of Video Teleconference was sent to the parties on September 4, 2020, notifying them of a hearing to be held on Monday, September 14, 2020.

Government Exhibits (GE) 1 through 4 and Applicant's Exhibits (AE) A through O were admitted into evidence. Applicant testified at the hearing, but did not introduce any additional documentary evidence or witnesses. DOHA received the hearing transcript (Tr.) on September 28, 2020.

Evidentiary Issues

On September 11, 2020, Department Counsel submitted a motion in limine to exclude AE C and D (comprised of AE C-private exculpatory polygraph examination report and AE D-private counterintelligence assessment). That same afternoon, Applicant's counsel requested, via email, an opportunity to submit a post-hearing response to the motion as the hearing was scheduled for the following Monday. No response was submitted since the motion was decided in Applicant's favor at the hearing. The video teleconference hearing was held as scheduled.

I denied Department Counsel's motion in limine at the hearing, and noted my intent to admit the documents in question into evidence, and to weigh them appropriately in my decision. In closing arguments, Department Counsel renewed his objection to the reports' conclusions. He argued that the documents were (1) impermissible hearsay, (2) that the credibility of the "experts" was not established, (3) that Applicant seeks to substitute the "expert's" judgment for that of the Administrative Judge, and (4) that the presentation of polygraph evidence goes beyond the Government's ability to present similar evidence because of the prohibition in previous versions of the DOD Credibility Assessment Program directive[1] on the acceptance of polygraph and credibility assessments (PCA) examinations or results from non-Federal PCA examiners.

[1] DOD Directive 5210.48 (April 24, 2015) (Incorporating Change 2, Effective October 1, 2020). Department Counsel argued that the 2015 version provided that "DOD Components shall accept only Polygraph and

The two exhibits in question include a letter report entitled "Polygraph Examination of [Applicant] Conducted on November 22, 2019" and curriculum vitae (CV) from a private practice polygraph examiner (AE C), and a document entitled "Counterintelligence Assessment" (AE D). AE C was prepared by the Director of Quality Control Standards and Regulations (Examiner), for a private polygraph examination company, employed since September 2019. He also noted he holds a current position as a "federal contract polygraph examiner" for another private company since July 2018, stating he performs counterintelligence polygraphs for DOD and the Naval Criminal Investigative Service (NCIS).[2] The examiner previously served as a polygraph examiner for another company, and as a counterintelligence and security officer for DOD and the Central Intelligence Agency (CIA) from 2008 to 2018.

AE D was prepared by a private consultant who briefly described himself as an "expert consultant"; a graduate of the United States Naval Academy; U.S. Marine Corps veteran; and Federal Bureau of Investigation (FBI) Special Agent since 1997, specializing as a counterintelligence specialist and behaviorist. He noted his "advanced training and experience in the area of social psychology and the practical application of the science behind relationship development and trust." He also stated "I ultimately lead (sic) the FBI's elite Behavioral Analysis Program." It is unclear whether the consultant is still an FBI employee.

Neither party produced the polygraph examiner or counterintelligence consultant to testify at the scheduled hearing.

Private Exculpatory Polygraph Report

The polygraph examination report (AE C) included a section labeled "preparation & interview phase," comprised of a narrative of an initial oral brief Applicant provided to the examiner and a narrative of Applicant's responses to a pre-test interview conducted by the examiner. In general, Applicant discussed the facts related to his company's investigation of his use of a company computer to view pornography.

The second section is labeled "testing phase," which included the test objective, test procedure, and relevant test questions. Three questions were asked related to Applicant's answers on his September 2017 SCA. The questions included:

Credibility Assessments (PCA) examinations and/or results of such examinations that are conducted by Federal PCA examiners." The 2018 and 2020 versions of the Directive eliminated this language.

[2] DOD Instruction 5210.91 provides that "DOD polygraph examiners and PCASS [Preliminary Credibility Assessment Screening System] operators shall neither perform examinations nor participate in PCA-related activities in connection with non-duty employment. DoD Components authorized to conduct PCA examinations may grant exceptions on a case-by-case basis, when there is no conflict of interest." Although the examiner's CV indicates that he is a current Federal contract polygraph examiner, no information was provided as to his Government approval for non-duty employment and a review of his conflict of interest status.

1. When you filled out the e-QIP we discussed, was your purpose to hide that investigation from future employers?

2. When you filled out the e-QIP we discussed, were you purposely trying to prevent disclosure of that investigation?

3. When you filled out the e-QIP we discussed, did you deliberately falsify your answer about the introduction of unauthorized media?

Applicant answered "no" to each question.

Finally, the last section labeled "evaluation phase," which is comprised of the examiners technical analysis of the test data, and his "professional opinion" as to the Applicant's truthfulness. The examiner concluded that Applicant had "no significant response," and opined that the Applicant was "truthful."

Polygraph examinations are widely used within the Government and serve a useful function when combined with other information to form an opinion as to the credibility of an applicant. In security eligibility cases, they may not be a substitute for the evaluation and judgment of the administrative judge in light of the totality of the evidence.

In DOHA hearings, relevant and material evidence may be received into evidence subject to rebuttal, and technical rules of evidence may be relaxed to permit the development of a full and complete record. Directive, Additional Procedural Guidance, § E3.l.19.[3] Unlike military courts-martial,[4] there is no *per se* rule against the introduction of private polygraph examination results by applicants in DOHA hearings.[5] In some states, introduction of polygraph evidence in criminal cases is barred by statute, while in others, it is expressly permitted. Within the parameters of law and regulation, an applicant in DOHA proceedings has the right to seek to present polygraph evidence that he or she believes is relevant and material to a defense to the Government's case against the applicant. ISCR Case No. 96-0785 (App. Bd. Sep. 3, 1998) However, polygraph evidence is not universally accepted as reliable. *United States v. Scheffer*, 532 U.S. 303 (1998). In *Scheffer*, the Supreme Court noted that there is simply no consensus that polygraph evidence is reliable. To this day, the scientific community remains extremely polarized

[3] The [Appeal] Board has cautioned against a strict application of the Federal Rules of Evidence in these proceedings. *See e.g.* ISCR Case No. 97-0202 (January 20, 1998) at p. 2. ISCR Case No. 96-0785 (App. Bd. Sep. 3, 1998).

[4] *United States v. Scheffer*, 532 U.S. 303 (1998). (The case presented the question whether Military Rules of Evidence (MRE) 707, which makes polygraph evidence inadmissible in court-martial proceedings, unconstitutionally abridges the right of accused members of the military to present polygraph evidence to rebut an attack on the accused credibility. The Court held that the exclusion of such evidence does not violate the accused's right to present a defense under the Sixth Amendment of the U.S. Constitution.)

[5] As noted by the DOHA Appeal Board, the [*Scheffer*] Court did not pass judgment on the accuracy, reliability, or fairness of polygraph tests, and, the Administrative Judge is required to consider whether an applicant seeking to present polygraph evidence demonstrates its accuracy, reliability, and fairness. ISCR Case No. 96-0785 (App. Bd. Sep. 3, 1998).

about the reliability of polygraph techniques. *Scheffer* 532 U.S. 303 at 309 (citations omitted).[6]

The *Scheffer* Court reviewed some of the scientific literature on the reliability of the polygraph exam, citing one study which found polygraph assessments of truthfulness to be "little better than could be obtained by the toss of a coin." *Scheffer* 532 U.S. 303 at 310. Although the *Scheffer* Court noted that most jurisdictions banned polygraph evidence altogether, it also cited some Courts of Appeals which left exclusion of such evidence to the discretion of district courts under the Supreme Court's *Daubert* test for the admissibility of expert testimony. The Court noted however, "[w]hatever their approach, state and federal courts continue to express doubt about whether such evidence is reliable." *Scheffer* 532 U.S. 303 at 312 (citations omitted).

Because of the unique nature of polygraph evidence, the Federal courts have recognized the need to consider various issues raised by polygraph evidence when the parties have not stipulated to its admissibility and when a *per se* bar does not exclude the evidence. Those issues include but are not limited to:

> (1) Are the results of the polygraph test relevant and material to the issues of the case?
>
> (2) Is the probative value of the proffered polygraph evidence outweighed by the amount of time and resources that would be needed to decide its admissibility?
>
> (3) Has the party proffering the polygraph evidence given the other party sufficient notice to adequately prepare to respond to the proffered polygraph evidence?
>
> (4) Has there been a showing that a proffered witness is qualified to give testimony about the reliability of polygraphs?
>
> (5) Has there been a showing that there is validity and reliability to polygraph examinations?
>
> (6) Has there been a showing that the polygraph examination in question was conducted by a qualified polygrapher, using proper techniques, in a proper manner?
>
> (7) Is the proffered polygraph evidence complete?

(Citations omitted); ISCR Case No. 96-0785 (App. Bd. Sep. 3, 1998)

[6] *Scheffer* was decided by a divided Court. A four-justice plurality and four-justices concurring, with one dissent, held that the military exclusion of polygraph results did not unconstitutionally abridge the accused's rights. Four Justices were not convinced that polygraph test results should be excluded in the federal system because of concerns over usurping the jury's responsibility to decide ultimate issues in the case. Eight Justices agreed with the statement raising doubts about the scientific community's acceptance of the reliability of polygraph techniques.

Federal criminal courts have questioned the admissibility and probative value of private polygraph examinations, and have expressed concern about trials "devolving into an evidentiary free-for-all." *See, e.g., United States v. Catalan Roman*, 368 F. Supp. 2d 119 at 121 (D.P.R. 2005). For example, after reviewing a district court's extensive analysis of the reliability of polygraph evidence, the U.S. Court of Appeals for the Ninth Circuit agreed that the defendant's private polygraph evidence did not satisfy the *Daubert* standards, and was therefore inadmissible. *United States v. Cordoba*, 194 F.3d 1053 (9th Cir. 1999); cert. denied, 2000 U.S. LEXIS 2804 (2000).

The U.S. Court of Appeals for the Eighth Circuit noted in 2011:

> Results from a unilateral polygraph examinations [sic] have little probative value. See *United States v. Sherlin, 67 F.3d 1208, 1217 (6th Cir. 1995)* (concluding that the defendant's "privately commissioned polygraph test, which was unknown to the Government until after its completion, is of extremely dubious probative value"). The defendant has no adverse interest at stake because a polygraph examination administered without notice to and participation by the Government "carries no negative consequences, and probably won't see the light of day if a defendant flunks." (citation omitted) Applying the balancing test set forth in *Federal Rule of Evidence 403*, courts have routinely deemed inadmissible, evidence related to unilateral polygraph examinations. (citation omitted) Moreover, the admission of the proposed evidence would have necessitated collateral proceedings regarding the validity of a unilateral polygraph examination. Accordingly, the polygraph evidence was properly excluded. *United States v. Montgomery*, 635 F.3d 1074, 1094 (8th Cir. 2011)

Even in Federal criminal cases in which the penalty is far more ominous than in DOHA cases, exculpatory polygraphs have been excluded. For example, a defendant in the capital-sentencing phase of his trial after convictions for conspiracy, armed robbery, and murder was denied the use of polygraph results that he asserted would clear his participation in the robbery. The Court clearly summarized the law regarding polygraph evidence in that District, noting that the Eighth Amendment guarantee to a capital defendant to present relevant mitigating information is not without its limits. Despite statutorily relaxed rules of evidence in capital sentencing proceedings[7] similar to regulations governing DOHA hearings, the Court stated that the "trial judge retains his traditional role as gatekeeper" and "must accordingly exclude any unreliable or prejudicial information that might render a trial fundamentally unfair." The Court also noted that "[p]olygraphs remain nearly universally frowned upon as courtroom lie detectors," and instead relied on the jury as the "lie detector," and reiterated that "there is simply no way to know in a particular case whether a polygraph examiner's conclusion is accurate because certain doubts and uncertainties plague even the best polygraph exams." *Catalan Roman* 368 F. Supp. at 122, *citing Scheffer* 532 U.S. 303 at 312. The Court held

[7] 18 U.S.C. 3593 (c) (Information is admissible regardless of its admissibility under the rules governing admission of evidence at criminal trials except that information may be excluded if its probative value is outweighed by the danger of creating unfair prejudice, confusing the issues, or misleading the jury.)

that "[p]olygraph results are inherently unreliable and this alone warrants their exclusion." *Catalan Roman*, 368 F. Supp. 2d at 124.

Although DOHA cases do not normally implicate such life or death consequences, and juries are not a part of our proceedings, such cases as those noted above reflect the Federal Courts' willingness to exclude favorable exculpatory polygraph evidence despite the degree of personal peril faced by defendants.

In this case, Department Counsel's main objection relates to the section of Applicant's polygraph report labeled "evaluation phase." I note that the exhibit does not contain technical charts or raw data; the report is silent on the use of control questions (although the report claims to have used "Federally authorized testing format and questions"); no audio or video recording of the interview and polygraph examination was disclosed; there is no listing of documents provided to the examiner or reviewed before the exam; and there was no evidence submitted that the technical data was reviewed by a quality control supervisor and a final opinion rendered, similar to that required for Government polygraph exams. *See* DOD Instruction 5210.91, March 30, 2020, at pp. 19-21. Inclusion of this information in the proposed exhibit would have provided the Government an opportunity to fully examine the information and obtain an expert's analysis, and avoid excessive time and resources that would be needed to decide its admissibility and reliability.

In addition, private polygraph examinations are generally a product prepared by, sold to, and paid for by individuals and their counsel. The private examiner is in the business of profiting from the exam and presumably anticipates future sales. Therefore, the private examiner's motivations may render the exams' results inherently, if unwittingly, biased in favor of the paying client. Of note, no evidence regarding bias or lack thereof was presented in this case. It should be noted when discussing private polygraph exams in general, results that go against the defendant or applicant's interests never "see the light of day" in a courtroom or DOHA hearing, so the Judge may never know how many private polygraph exams were "failed" before considering the favorable exam submitted.[8]

The extent to which Government-obtained polygraph evidence is used in security eligibility determinations must be considered. Polygraph technical analysis alone is not generally acceptable as definitive evidence of truthfulness or untruthfulness. Government clearance decisions comprising statements of fact an applicant made during pre- or post-test interviews connected with polygraph examinations are generally admissible as substantive evidence in DOHA hearings. *See, e.g.*, ISCR Case No. 07-18324 at 5 (App. Bd. Mar. 11, 2011). The Government may not take adverse action solely on the basis of polygraph examination technical calls in the absence of adjudicatively significant information." SEAD 4: National Security Adjudicative Guidelines (December 10, 2016), Appendix A, ¶ 1(c).

[8] There is no evidence in the record, nor do I have reason to suspect, that Applicant took more than one polygraph examination or that he "failed" any previous polygraph exams.

The DOHA Appeal Board has noted that:

> The oral or written statements made by the subject of a polygraph examination are not the same as the polygraph charts, or the polygrapher's opinion whether the subject's statements are truthful or deceptive. The reliability or unreliability of the polygraph machine, a polygrapher's interpretation of a polygraph chart, or a polygrapher's opinion as to the veracity of a person undergoing a polygraph examination are factually and legally distinct from the statements a person may make during or after a polygraph examination. *See also* ISCR Case No. 94-1057 (August 11, 1995) at p. 6 (citing *Wyrick v. Fields*, 459 U.S. 42, 48 n.* (1982) and noting the difference between a polygraph examination chart and an applicant's post-polygraph statements).

ISCR Case No. 02-31428 (App. Bd. Jan. 20, 2006) at p.4. *See also* ISCR Case No. 11-03452 (App. Bd. Jun. 6, 2012) (involving analysis of evidence that Applicant used polygraph countermeasures).

Likewise, conclusory opinions of private polygraph examiners, based on technical analysis alone, should be viewed with skepticism as to the accuracy of the polygraph examination and analysis of data and interpretation of physiological reactions, and should not be accepted as determinative of the matter examined. However, testimony in the form of an opinion or inference otherwise admissible is not objectionable even if it embraces an ultimate issue to be decided by the trier of fact. ISCR Case No. 96-0785 (App. Bd. Sep. 3, 1998)

I find that the polygraph examination report (AE C) is minimally complete, and the probative value of the "evaluation phase" of the report was not outweighed by the amount of time and resources that would be needed to decide its admissibility. The addition of the deficient items as part of the report would have aided in evaluating the credibility, reliability, and accuracy of the examiner's analysis and conclusions, but the possibility of inherent bias of the private polygraph examiner must also be considered. Although the report was admitted on its face, the administrative judge must determine the appropriate weight to be applied. The Appeal Board noted:

> It is not unusual for a Judge to be faced with the need to consider and weigh conflicting record evidence. A Judge faced with conflicting record evidence must decide how much weight to give to the conflicting pieces of record evidence and make findings of fact that reflect a reasonable interpretation of the record evidence as a whole. *See e.g.*, ISCR Case No. 02-09892 (July 15, 2004) at p. 5. A Judge must – of practical necessity – weigh the record evidence, decide what evidence is credible and persuasive, and make findings of fact concerning controverted factual issues. ISCR Case No. 02-31428 (App. Bd. Jan. 20, 2006).

Accordingly, I have considered the entire polygraph report (AE C), including the report's narrative "preparation & interview phase" and the Applicant's responses to specific questions in the "testing phase" and the "evaluation phase." I give little persuasive value to the "evaluation phase" of the report, as the examiner's data interpretation, opinions and conclusion are not conclusively determinative of the issues addressed in the report and do not serve to outweigh other record evidence.

Private Counterintelligence Assessment

Applicant's privately obtained counterintelligence assessment report (AE D) is problematic in several areas. First, the qualification of the "expert" consultant (assessor) is not fully developed. Although the expert was "retained" by Applicant's counsel to prepare a counterintelligence assessment, it is unclear whether the assessor is still a Federal employee or in the business of preparing assessments for profit. Next, the report does not fully develop the expert's qualifications, including specific education and training, and the length and specificity of experience. Rather, the totality of the expert's qualifications in counterintelligence was summarized in two sentences after he noted that he was a Naval Academy graduate and former U.S. Marine Corps officer. The paucity of the consultant's education and background information appears to assume that a college degree and some military and FBI experience is sufficient to qualify him as a counterintelligence expert, and thus, gives his opinion appropriate gravitas.

The expert reviewed documents that were eventually admitted into evidence at the hearing, presumably including the polygraph examiner's data analysis, opinions, and conclusion as noted above. The expert interviewed Applicant via a video teleconference; however, he did not provide a transcript or summary of the interview despite claiming it to be a factor he used to develop the basis for his assessment. The expert concludes that Applicant "does not pose a security risk" and that Applicant "demonstrates characteristics of an individual who is trustworthy, and who is able to maintain classified information without significant risk of compromise by bad actors or foreign intelligence agents." The basis for this conclusion is not adequately addressed in the report, despite the expert's reliance on his "21 years of experience working insider threat and espionage investigations."

Additionally, the expert did not mention the consideration or weight applied to the behavior that formed the basis of the SOR in the formation of his opinion of Applicant's trustworthiness and potential for compromise. Notably, no mention was made in the report regarding the inherent risks Applicant willingly took to introduce a personal hard drive containing pornography into a company laptop that would be connected to company information system, as an avenue to place malicious computer code into a computer system or network. However, the expert appears to give great weight to Applicant's past involvement with classified and special access (SAP) programs as a defense contractor.

He reasoned that since Applicant's knowledge of classified information is "front loaded" when he first obtained a clearance or was "read into" a program, the "most significant risk to national security has already taken place." The expert inexplicably noted

that with Applicant's continued access to classified information and his current SAP program, there is not "much added risk to national security." This is not the evaluative process mandated by the Directive.

Finally, the expert concluded his assessment by again stating that it is based on his "knowledge, experience, and training," and is "no guarantee of future behavior or future security of information." Given the skeletal nature of the report, it is difficult to find value in or rely on its conclusions.

Although I admitted the counterintelligence assessment into evidence and fully considered its content, I find it to have little to no persuasive value as it does not meaningfully or persuasively contribute to a determination of Applicant's trustworthiness, judgment, or security worthiness.

Findings of Fact

Applicant is a 44-year-old senior program manager for a defense contractor, employed since August 2017. He previously worked as a senior staff project engineer for another defense contractor from 2001 until he was suspended and resigned in June 2017. He received two bachelor's degrees in 1998 and 2000, a master's degree in 2004, and a doctorate degree in 2013. He married in 2000 and has four children, ages 10 through 17. He testified that he has held DOD security clearances and special access program (SAP) privileges for over 19 years. He reported that his top-secret clearance was granted in about 2003.

The SOR alleges under Guideline M (Use of Information Technology) that Applicant resigned in June 2017 in lieu of termination after his employer discovered that he misused a company computer to view pornography or adult-oriented material, and he violated security protocols by using a personal external storage device on a company computer.

The SOR alleges under Guideline E (Personal Conduct) that: (a) Applicant falsified his September 2017 SCA by answering "no" to a question in Section 13C - Employment Record, asking if he was fired from a job; quit after being told he would be fired; left a job by mutual agreement following charges or allegations of misconduct; left a job by mutual agreement after notice of unsatisfactory performance; received a written warning, been officially reprimanded, suspended, or disciplined for misconduct in the workplace, such as a violation of security policy; and (b) Applicant falsified his September 2017 SCA by answering "no" to a question in Section 27 – Use of Information Technology Systems, asking if he introduced, removed, or used hardware, software, or media in connection with any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines, or regulations, or attempted any of the above.

In his Answer to the SOR, Applicant admitted that he used his work-issued laptop to view sexually-explicit videos at his home with his wife. He claimed that on five to ten occasions, he inserted a removable drive that contained sexually-explicit videos into a

USB port on his company laptop to view with his wife. He denied that he resigned from his job in lieu of termination; rather he averred that although he knew his actions could result in "future disciplinary action," he resigned because he was embarrassed and his reputation was tarnished at his workplace. (Ans.)

Applicant also denied falsifying his SCA, claiming he did not resign under an "explicit or promise of future discipline" or for any other reason posed in the question 13C on his SCA, and that an answer of "no" continues to be the correct answer. He also stated that although his initial answer to SCA question 27 was "factually incorrect," he did not deliberately falsify his answer. He explained that he corrected his answer to question 27 after reviewing it with the investigator during his personal subject interview (PSI), and that he was "open and candid with the investigator about his reasons for leaving" his employment. (Ans.) In fact, the PSI shows that Applicant was twice asked about his response to SCA question 13C regarding his suspension from employment, not question 27 regarding his use of information technology (IT) systems, where he changed his SCA answer and admitted the violation. (GE 2.)

Applicant's work for his previous employer, a defense contractor, spanned 16 years and required security eligibility at the top-secret level, with special access program privileges. He was a first-line manager and supervised other cleared employees. He was trained on information security measures while employed with the company, and attended required security briefings. He worked within a DOD-designated "closed area" where phones, personal computers, and other personal devices were prohibited, however company-issued laptops were allowed into the area and were connected to company IT systems while there. Before the incidents in question, Applicant had no prior security infractions.

Applicant used his work-issued computer to view pornography installed via a personal USB device (external hard drive). He testified that he used the USB device and company computer to view pornography for four to six months, including with his spouse and while on travel alone. He did not correct the length of time he used the device when speaking to the government investigator, nor did he correct it on his PSI when he certified its accuracy in response to Government interrogatories.

When the USB device was inserted into the computer, a warning banner appeared on the screen that warned about moving information to or from the computer. Applicant admitted in his PSI that he knew of the policy prohibiting employees from inserting external non-employment-approved hardware into work devices (GE 2.), but later testified that the use of a personal USB device plugged into the computer was a "grey area." (Tr. 38) Applicant justified his actions by claiming that he was not logged into a company network, he was not on duty, and the computer was not used for classified work. He testified that he knew viewing pornography on his company computer was a violation of company policy. (Tr. 38; AE L.)

Unbeknown to Applicant, his company computer was being monitored by his employer, who discovered the improper activity and conducted an investigation. (GE 2;

GE 4.) The company's investigation revealed that pornography was present on Applicant's USB drive and that using a company computer to view such material was prohibited. (GE 4.) The investigator explained to Applicant that pornography was a "commonly recognized threat vector" and a method for "placing malicious computer code into a computer system or network." (GE 4.) Applicant confirmed that he also used the USB device while on a recent business trip, and admitted that he used "absolutely incredibly poor judgment in using the device." (GE 4.)

Applicant also used the work computer to access an online website to view online personal ads while on travel, and used "email to look for a meeting with other men." (GE 4.) Applicant told the investigator that he was only "playing a game," and that no meeting occurred on his last trip, but admitted that he previously met with people on two other occasions but never discussed his work and had no continuing contact with either person. (GE 4.) The company investigator explained to Applicant that "engaging in such activity could place him at great risk physically and professionally by someone he met by attempting to harm or compromise him in some manner." (GE 4.) Applicant's use of the company computer to arrange personal liaisons was not alleged in the SOR.

Applicant carried his personal USB device into the closed work area in his briefcase, in violation of company policy. (GE 4; AE L.) The company labeled this a security violation. (AE L.) Contrary to his testimony, he admitted to the company investigator that he knew using the USB device in his company computer was prohibited, but he claimed he was "not sure" whether the device could be carried into the closed work area. (GE 4.) In testimony, he stated that he did not know he was prohibited from taking the device into the closed area, but he "should have known." (Tr. 34-37.) Introducing a prohibited device into the closed work area was not alleged in the SOR.

In a subsequent statement addressed to the company disciplinary review board (DRB), Applicant stated that he "exercised some very poor judgment in [his] personal life and does not dispute any of the facts as presented to [him] by the investigators." (GE 4 – Statement.) He pleaded with the DRB that he would accept any disciplinary action mandated if they allowed him to continue employment, but if that was not possible, he requested that the DRB allow him to resign or impose a form of termination that might allow him a clean start in another industry. (GE 4 – Statement.)

Applicant was stripped of his access badge and was placed on indefinite disciplinary suspension pending a formal disposition of the DRB. (GE 4; AE L.) The company reported Applicant's conduct to DOD via a JPAS incident history report, and noted that Applicant resigned via email on June 22, 2017, the day before the DRB. The company noted that Applicant's resignation was "in lieu of termination," and he was not eligible for rehire. (GE 3; AE L.) Applicant was aware that the DRB could result in disciplinary action or termination of employment, and testified that he was concerned about his reputation in the company and believed a "negative" DRB outcome would limit his ability to retain a security clearance. (Tr. 21-26.) In testimony, he quibbled regarding the labeling of his suspension, calling it "administrative leave," not a suspension, because he was not formally notified of a suspension and was paid. (Tr. 41.)

Applicant was interviewed by a Government investigator in August 2018 (PSI) while he was employed by another defense contractor. He did not initially reveal his suspension and full involvement in the misuse of the company computer. He was twice asked if he had received a written reprimand, been officially reprimanded, suspended, or disciplined for misconduct in the workplace such as a violation of security policy, and he twice answered "no." When confronted with his suspension from his previous employer, he hesitated before admitting that he was suspended for inserting personal hardware into his work computer to view pornography. (GE 2.)

When asked by the investigator whether he introduced, removed or used hardware, software, or media in connection with any information technology system without authorization when specifically prohibited, he stated "yes." He claimed he misunderstood the related question on his SCA when he answered "no" to question 27, but did not elaborate on what he misunderstood. (GE 2.) In testimony, Applicant claimed that he answered "no" to question 27 because he believed the question was limited to classified systems, despite that it specifically referred to "any information technology system." (Tr. 27-29.) He testified that he finally understood that his answer on the SCA was incorrect after the investigator repeated the question with an emphasis on "any" system. I note that the PSI does not indicate that Applicant was coached by the investigator or that the investigator had to emphasize any particular part of SCA question 27, rather the investigator noted that she twice asked Applicant to disclose his employment record in response to SCA question 13C, before he acknowledged his suspension.

Applicant explained to the Government investigator that he used the USB and computer to view pornography with his wife in their bedroom, but he did not disclose that he also used it while alone on a business trip, or that he searched personal ads, used email to arrange liasons while traveling, or that he introduced the prohibited USB device into a closed work area in violation of security regulations and company policy. (GE 2.) He acknowledged in his interview that he was aware that inserting his personal USB into the computer to view pornography was prohibited, and claimed, contrary to his hearing testimony, that he did so "many times in a month to two months timeframe." (GE 2.) Applicant acknowledged that his misuse of the computer violated company policy and took full responsibility for his actions. He claimed he had a "terrible lapse of judgment" and became "impulsive." He explained that he did not disclose his conduct on his SCA because he interpreted the question (SCA question 27) as strictly related to violating "security policies." (GE 2.)

Applicant disputes that he was "suspended" and resigned in lieu of termination or by mutual agreement. Applicant testified that he was not formally suspended, rather he was simply on paid administrative leave. He also testified that he did not resign by mutual agreement or in lieu of termination because he resigned the day before the DRB was scheduled to meet, and he was not told he would be fired. However, in his PSI, he admitted that he was "suspended with pay for a week." (GE 2.) He further explained in his PSI that he "was told that he was being suspended for [a] week pending the disciplinary board's decision. [Applicant] went home on paid suspension and after a week,

he resigned. He was not told he would be fired but he was afraid of having his security clearance revoked by the disciplinary board." (GE 2.) Applicant did not change or correct this language when he verified the PSI's accuracy in response to an interrogatory.

In SCA question 13A regarding Applicant's employment history, he was asked for the reason he left employment. Applicant answered that he "resigned to take position at [another defense contractor]." (GE 1. p.14.) In addition, when asked if he left employment by "mutual agreement following charges or allegations of misconduct" or "following notice of unsatisfactory performance," Applicant answered "no." (GE 1. p.14.) However, Applicant did not have a new position with his current employer at the time he resigned. (Tr. 48.) He testified that after resigning, he contacted a program director with another government contractor whom Applicant met while conducting business with his previous employer. According to the program director that conducted the interview, Applicant disclosed that he made a "personal mistake and had inappropriately used an unclassified [company]-owned laptop computer. As a result of that incident, he was personally embarrassed and felt that the incident would have lasting negative impact on his ability for career advancement" with the company. (AE E.) The new employer concluded that Applicant had a "significant lapse in judgment and that it violated [his company's] policy, it was not a security infraction." Applicant was hired in the summer of 2017, and is currently employed in substantially the same classified work he performed with his previous employer. The evidence is unclear as to what, if any, other information was provided to the new employer regarding Applicant's previous employment conduct, and on what basis it determined that Applicant's actions did not qualify as a "security infraction."

In his PSI, Applicant acknowledged his lack of judgment when using the company computer, and attributed it his "ignorance and careless actions." (GE 2.) He took accountability for his "mistake" and learned a lifelong lesson. He avers that he hopes to put the incident behind him, but asserts that use of the USB device in the computer "did not put the company's security at risk and no data or PII was lost. (GE 2.) Of note, Applicant continued to under report the extent of his use of the USB and company laptop when he completed an "Affidavit of [Applicant]" in April 2020. In the affidavit, he admitted to violating company rules by viewing the pornography with his wife, but failed to disclose his use while on travel. (AE J.) He also continues to deny that he has breached any security protocols by stating "for all of my 19 year career, I have not had single [sic] infraction or incident involving any security issues."

In a review by Applicant's former employer, they noted in a letter dated June 11, 2020 that:

> When [the company] representatives interviewed [Applicant], he admitted to viewing the materials using his [company] asset and understanding that such actions were prohibited. As such, [Applicant] was placed on an indefinite disciplinary suspension pending formal determination by the Disciplinary Review Board (DRB). [Applicant] was offered the opportunity to provide a written statement, which he did. In that statement, [Applicant]

> admits to the misconduct, stating, 'I am not attempting to defend or justify my actions in any way . . .' and, 'I know I'm in no position to ask for favors and will accept whatever decision [the DRB] reache[es].' On June 23, 2017, the date the DRB was scheduled to meet, [Applicant] tendered his resignation.
>
> In light of the nature of the substantiated misconduct, [Applicant's] Top Secret clearance, and resignation while on a disciplinary suspension, [the company] appropriately coded [Applicant's] resignation as a 'resignation in lieu of termination.' Such is consistent with [the company's] policy and procedures, and its obligation as a federal contractor and applicable law. (AE L.)

Applicant's current employer fully supports him, has promoted him to manage a highly-classified sub-product line that generates $125 million in annual sales, highlighted his accomplishments, trustworthiness, and importance to the company and to the U.S. national defense industry. The employer notes that they do not have another leader of Applicant's caliber waiting in the wings to replace him. (AE E.)

Likewise, Applicant's former coworkers expressed their strong support for him and discussed the harm that would occur to his new employer and the Government if Applicant does not retain his security clearance and continue work on important, highly-classified projects. (AE F, G.) Applicant's spouse also supports him and acknowledged that their use of the company computer to view pornography together was an "egregious error." (AE H.)

Policies

"[N]o 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 applicants 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 § 2.

National security eligibility is predicated upon the applicant meeting the criteria contained in the adjudicative guidelines. These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, an administrative judge applies these guidelines in conjunction with an evaluation of the whole person. An administrative judge's overarching adjudicative goal is a fair, impartial, and commonsense decision. An administrative judge must consider a person's stability, trustworthiness, reliability, discretion, character, honesty, and judgment. AG ¶ 1(b).

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 about potential, rather than actual, risk of compromise of classified information.

Clearance decisions must be made "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." Exec. Or. 10865 § 7. Thus, a decision to deny a security clearance is merely an indication the applicant 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. *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 therein and an applicant's security suitability. *See, e.g.,* ISCR Case No. 12-01295 at 3 (App. Bd. Jan. 20, 2015).

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 burden of proving a mitigating condition, and the burden of disproving it never shifts to the Government. *See, e.g.,* ISCR Case No. 02-31154 at 5 (App. Bd. Sep. 22, 2005).

An applicant "has the ultimate burden of demonstrating that it is clearly consistent with the national interest to grant or continue his security clearance." ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002). "[S]ecurity clearance determinations should err, if they must, on the side of denials." *Egan*, 484 U.S. at 531; *see,* AG ¶ 1(d).

Analysis

Guideline M: Use of Information Technology Systems

AG ¶ 39 expresses the security concern pertaining to use of information technology systems:

> 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.

Relevant conditions that could raise a security concern under AG ¶ 40 and may be disqualifying include:

(e) unauthorized entry any information technology system; and

(f) introduction, removal, or duplication of hardware, firmware, software, or media to or from any information technology system when prohibited by rules, procedures, guidelines, or regulations or when otherwise not authorized.

The evidence presented is sufficient to raise the security concerns described above.

Conditions that could mitigate security concerns arising from incidents regarding use of information technology are provided under AG ¶ 41. 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; and

(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.

None of the mitigation conditions fully apply. While the conduct in question that led to Applicant's resignation to avoid discipline or termination was discovered by the company in 2017, and had occurred numerous times up to six months prior to discovery, the conduct was knowing and intentional, and there is insufficient evidence that Applicant has taken full responsibility or that sufficient time has elapsed to show that it is unlikely to recur.

The conduct discussed in the findings of fact clearly display an ongoing pattern of intentional security and company policy violations and misuse of company resources that could jeopardize a government contractor's IT systems. Applicant attempted to evade culpability by resigning before the DRB could conclude its deliberations with the hope of avoiding discipline, termination, or the loss of security eligibility. He also falsified his SCA and was reluctant to disclose his actions to a government investigator without prodding. Finally, he provided incomplete and inconsistent explanations during the clearance process. His actions continue to cast doubt on his reliability and trustworthiness, and call into question his willingness to protect sensitive systems and networks.

Despite computer banner warnings displayed every time he wrongfully used the USB device, Applicant continued the computer activity for up to six months. He initially claimed he used the computer in this manner for one-to-two months, but he admitted at the hearing that it was actually four-to-six months. He did not correct the misinformation or incomplete information provided to the government investigator, nor did he correct the PSI when provided with the opportunity in response to interrogatories. Rather he certified the accuracy of the PSI. Applicant's willful misuse of the computer and USB device occurred while alone on business travel as well as with his spouse, a fact not disclosed to the government investigator. Applicant was disinclined to disclose his computer misconduct and suspension to the investigator without being confronted and prodded. He willfully failed to disclose his conduct and suspension in his SCA, and was evasive in reporting the reason for leaving employment. These behaviors display a reluctance to fully disclose and take responsibility for his actions, and an ongoing effort to minimize or divert his culpability.

Additionally, Applicant did not disclose information to the government investigator, regarding taking an unauthorized device into the closed workspace or misusing the company's computer and email to arrange personal liaisons while traveling. Although this conduct was not alleged in the SOR, it is appropriate to consider it:

> (a) to assess his credibility; (b) to evaluate his evidence of extenuation, mitigation, or changed circumstances; (c) to consider whether he has demonstrated successful rehabilitation; (d) to decide whether a particular provision of the Adjudicative Guidelines is applicable; or (e) to provide evidence for whole-person analysis. *See* ISCR Case No. 03-20327 at 4 (App. Bd. Oct 26, 2006).

A pattern of IT security violations and Applicant's willingness to engage in potentially compromising behavior refutes Applicant's claim of a regrettable transgression and plea for forgiveness and reform.

Applicant is a highly-educated and experienced supervisor, with a long history of work with IT assets in classified and sensitive environments. He acted in full knowledge of the risks and willfully ignored security training and computer banner warnings for personal pleasure. Depending on the forum, Applicant is quibbling and vague about the details of his actions and his knowledge of company rules and policies. He continues to show an unwillingness to grasp the gravity of his actions by claiming that he did not put the company's security at risk, despite the explanations and warnings given to him by the company investigator. No mitigating conditions fully apply.

Guideline E; Personal Conduct

AG ¶ 15 expresses the personal conduct security concern:

> 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 cooperate or provide truthful and candid answers during national security investigative or adjudicative processes.

AG ¶ 16 describes conditions that could raise a security concern and may be disqualifying in this case. The following disqualifying condition is potentially applicable:

> (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 national security eligibility or trustworthiness, or award fiduciary responsibilities; and
>
> (b) deliberately providing false or misleading information; or concealing or omitting information, concerning relevant facts to an employer, investigator, security official, competent medical or mental health professional involved in making a recommendation relevant to a national security eligibility determination, or other official government representative.

The personal conduct alleged is generally sufficient to implicate AG ¶¶ 16 (a) and (b).

Conditions that could mitigate security concerns arising from incidents of personal conduct are provided under AG ¶ 17. The following 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 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 contributed to 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.

I have considered all of the mitigating conditions under AG ¶ 17. Applicant engaged in a pattern of knowing and intentional deception when he failed to disclose in response to SCA section 13C - Employment Record, his suspension for misconduct including violations of company security policies, and his resignation by mutual agreement after

being notified of misconduct in the workplace such as a violation of security policies, or in lieu of termination, as labeled by his company. No matter how Applicant would like to mince words and obfuscate the reality of his employment situation, it is clear that he resigned in order to avoid serious disciplinary action including termination, and a critical finding by the DRB that would jeopardize his security clearance.

In addition, Applicant failed to disclose in response to SCA section 27 - Use of Information Technology Systems that he misused his company computer by inserting a prohibited USB device to view pornography, in violation of company rules, policies and procedures.

Although not alleged in the SOR, Applicant (1) intentionally failed to disclose the reason for leaving his last employment in response to SCA section 13A; (2) failed to disclose to a government investigator that he introduced a prohibited device into the closed workspace, a security violation; (3) used a company computer and email to view online personal ads and arrange for personal liaisons while traveling, a behavior that put him at personal and professional risk of harm or compromise; and (4) deliberately failed to voluntarily disclose his suspension during his PSI without being confronted or prodded. It is appropriate to consider this information to assess his credibility; to evaluate his evidence of extenuation, mitigation, or changed circumstances; to consider whether he has demonstrated successful rehabilitation; and in my whole-person analysis.

Applicant's behavior was serious, recent, and recurring. He was reluctant to correct the record without being confronted and prodded. He has not convincingly shown an understanding of the security ramifications of his conduct, or sincere remorse. Rather, he has displayed more concern for himself and the impact on his career and clearance eligibility. He failed to fully cooperate with government investigators and straightforwardly disclose the extent and details of his conduct. Rather, he has shown a propensity to minimize, equivocate, and obfuscate his conduct.

I am not convinced that Applicant's display of poor judgment, intentional falsifications, and lack of candor is behind him, or that similar conduct will not recur. After discovery of his conduct by his company, he attempted to avoid a detrimental DRB determination, then displayed a lack of honesty and candor by not providing full, frank and truthful answers during the security investigation process. Given the circumstances detailed above, I find that no mitigating condition fully applies and that Applicant's behavior overall warrants an unfavorable clearance action.

Whole-Person Concept

Under AG ¶¶ 2(a), 2(c), and 2(d), the ultimate determination of whether to grant national security eligibility must be an overall commonsense judgment based upon careful consideration of the guidelines and the 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(d).

I considered all of the potentially disqualifying and mitigating conditions in light of the facts and circumstances surrounding this case. I have incorporated my findings of fact and comments under Guidelines M and E, in my whole-person analysis. I also considered Applicant's long history of employment and security eligibility, his current employment circumstances, the importance of his skills and knowledge to his employer and the Government client, and the strong support from his family and coworkers.

Applicant was expected to conduct himself in a manner consistent with an experienced and knowledgeable senior defense contractor employee, and comply with IT security protocols and respect the security investigation process. However, his pattern of misconduct, lack of candor, and self-serving behavior does not overcome presumptions of mistake, ignorance, or an isolated event that may be due a person with an otherwise excellent employment record. I remain concerned about Applicant's continued trustworthiness to protect national security information and ability to comply with rules and regulations.

Accordingly, I conclude Applicant has not carried his burden of showing that it is clearly consistent with the national interest of the United States to grant him 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 M:	AGAINST APPLICANT
Subparagraph 1.a:	Against Applicant
Paragraph 2, Guideline E:	AGAINST APPLICANT
Subparagraphs 2.a and 2.b:	Against Applicant

Conclusion

I conclude that it is not clearly consistent with the national interest of the United States to grant or continue Applicant's eligibility for access to classified information. Applicant's security clearance is denied.

_____
Gregg A. Cervi
Administrative Judge