DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
[REDACTED]	)	ISCR Case No. 18-01178
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Bryan J. Olmos, Esq., Department Counsel
For Applicant: Mark A. Myers

03/31/2020

Decision

HESS, Stephanie C., Administrative Judge:

Applicant failed to mitigate the personal conduct security concerns raised by his past conduct and ongoing inconsistent statements. Eligibility for access to classified information is denied.

Statement of the Case

Applicant submitted a security clearance application (e-QIP) on November 1, 2016. On September 19, 2018, the Department of Defense (DOD) sent him a Statement of Reasons (SOR), alleging security concerns under Guideline E (Personal Conduct) and Guideline M (Use of Information Technology). The DOD acted under Executive Order (Ex. 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 adjudicative guidelines (AG) implemented by DOD on June 8, 2017.

Applicant submitted his Answer to the SOR on November 14, 2018, and requested a hearing before an administrative judge. Department Counsel was ready to proceed on December 30, 2018, and the case was assigned to me on June 7, 2019. On that same

day, DOHA notified Applicant that the hearing was scheduled for June 27, 2019. I convened the hearing as scheduled. Government Exhibits (GX) 1 through 9 were admitted into evidence. Applicant testified and Applicant Exhibits (AX) A through AX W were admitted into evidence. I left the record open until July 11, 2019, to enable Applicant to submit additional documentary evidence. He timely submitted AX X – AX AA, which I have admitted without objection. DOHA received the transcript (Tr.) on July 11, 2019.

Procedural Issues

Department Counsel offered into evidence GX 4 which is a report of investigation from Applicant's 2014 employer which formed the basis for Applicant's termination. The facts set forth in SOR ¶ 1.a were taken from the report. Applicant's attorney objected to my admitting the document because the document did not include the listed attachments and was therefore incomplete.

In ruling on this objection, I considered the following: The report sets forth the allegations against Applicant; the company's applicable policies; a synopsis of events; and the names of the involved individuals. In a section entitled "Details," the report sets forth a description of the events giving rise to the investigation; includes copies of two emails between Applicant and a contractor listed as an involved individual; delineates information from the audit logbook during the time of the incidents; and sets forth information from the system and application logs. The report also summarizes communications to and from the information security manager concerning the investigative process. The report sets forth its conclusions and states the basis for Applicant's termination. Finally, it is signed by the FSO. The listed attachments not provided with the document were "audit log printout," "email from [contractor]," and "email from [information security manager]."

I considered that the report was incomplete without the listed attachments, but determined that the report contained sufficient information to be admitted into evidence as a business record that was authentic, relevant, and material to determining Applicant's trustworthiness and gave the document its appropriate weight.

During the hearing, Applicant's attorney again objected to the report as incomplete and as inaccurate. Applicant testified at length regarding the report and I have considered both the document and Applicant's testimony in determining the appropriate weight to give the report.

Findings of Fact

Applicant is a 40-year-old senior cybersecurity engineer and security control assessor/validator currently employed by a defense contractor since December 2017. He has also been employed as a consultant part-time by another defense contractor since 2016. He received his high school general equivalency degree (GED) in 2002. Applicant enlisted in the Army in 2003 and served honorably on active duty until 2007. During his enlistment, he deployed to Iraq where he sustained significant injuries during combat in

2004. He has since been awarded a VA Disability Rating of 70%. Applicant served honorably in the Army National Guard from 2009 until 2012. He married in 2006 and divorced in 2009, and has an 11-year-old daughter from this marriage. Applicant was granted his first security clearance in 2008. (GX 1.)

The SOR consists of allegations under Guidelines E and M. Under Guideline E, ¶¶ 1.a and 1.b allege that Applicant was terminated from two employers, in part, for failure to perform audits as required by the National Industry Security Program Operating Manual (NISPOM). This conduct is cross-alleged under Guideline M, ¶ 1.a. The SOR allegations and Applicant's responses to them, are discussed more fully below.

SOR Allegations

Applicant was terminated from Company A in 2016 for failing to complete his job responsibilities

Applicant worked or Company A from January 2016 until August 2016 as a systems security manager. SOR ¶ 1.a stems from this employment. The SOR alleges:

SOR ¶ 1.a: Alleges:

You were terminated from your employment at [Company A] in about August 2016 for labor mischarging, which is a violation of [Company A's] code of ethics and business conduct, along with failing to complete mandatory NISPOM required audits.

In response to SOR ¶ 1.a, Applicant admits in his Answer that he was terminated from his employment in August 2016, but denies the alleged conduct that resulted in his termination. He states that despite his efforts to determine the reason for his termination, to include filing an ethics complaint (which was found to be without merit), he did not know the reason he was terminated until he received the Government's discovery. He further contends that the fact that he successfully claimed unemployment benefits is evidence that he was not terminated for cause. Additionally, he denies overcharging his hours, stating "my pay was always correct, if I had falsified my timecard my paycheck should have been different or changed." He supports this statement by providing copies of his May to September 2016 bank statements. (AX L.)

An August 8, 2016, JPAS incident report states an internal investigation into Applicant's conduct was underway because software patches were not completed as necessary, audits were not performed weekly, and there was potential adverse information concerning timecards. (GX 5.)

The Government presented a January 24, 2017, letter from Applicant's former employer's facility security officer (FSO) to DSS. (GX 7.) The letter that states that the internal investigation concluded that Applicant "was consistently over reporting time

worked." The conclusions of the investigation were "based on badging data and video evidence that was obtained from our Security Operations Center along with network login data and cell phone records obtained from our Incident Response Team." The investigation also concluded that Applicant had "failed to conduct mandatory NISPOM required audits and software updates on classified systems." The letter also noted that "all auditing and software updates have been completed and it was determined that there was no loss or compromise of classified data due to this finding." (GX 7.)

Applicant described his job responsibilities as "the facility security officer, [community security] custodian, the information system security manager, the offsite program manager, that was it." (Tr. 90.)

Based on the findings of the investigation, Applicant's employer determined that Applicant was in violation of its code of ethics and business conduct and NISPOM requirements and terminated Applicant in August 2016. The letter also stated that all auditing and software updates had since been completed and that no classified material had been compromised. (GX 7.)

Applicant refutes the findings of investigation set forth in the January 2017 letter. He testified that he completed all audits as required and that he properly reported his hours. (Tr. 30-31.) He also stated that the fact that he was eligible for unemployment benefits is evidence that he was not fired for cause. (Tr. 30.)

Applicant presented a May 3, 2019, letter from a former off-site FSO of the 2016 employer to refute the Government's evidence. The former FSO worked for the 2016 employer January 2006 until January 2019. Her tenure included Applicant's period of employment. She did not directly supervise Applicant in his FSO responsibilities, but he did report to her department. She stated that he did not have any security incidents or violations and that he successfully passed two Defense Security Service (DSS) audits. DSS routinely conducts security vulnerability assessments to assess compliance with the provisions of NISPOM and evaluate facilities' programs for protecting classified information in compliance with current directives. (AX M.) The former FSO further stated that she had known Applicant for five years and strongly recommends continuing his security clearance. (AX W.)

The former FSO states that she reviewed the January 2017 letter and states "with a degree of certainty that the evidence collected against [Applicant] could not be possible for the following reasons:

1) The closed area (classified workspace) where Applicant worked did not have badging capabilities;

2) The closed area contains classified materials, and there are no video recording devices within the facility for this reason;

3) The closed area contains a classified network that is not connected to the Internet. It would not have been possible to obtain Applicant's login data records because there is no external connection;

4) The employer did not allow company applications, to include email, on personal mobile devices, therefore it would not have been possible to obtain Applicant's personal cell phone records.

The former FSO also states that she prepared for a DSS audit immediately following Applicant's termination, although she does not specify the date the audit was performed. She states that when she conducted the audit, it showed that all required audits had been properly completed and were in compliance with NISPOM, and that there were no missing software updates.

Applicant testified that the employer installed a badge reader on an external door shortly before Applicant's termination. (Tr. 94.) Additionally, he also stated that he was required to log in to the company's internal network to utilize the company's email. (Tr. 130.)

Applicant was terminated from Company B in 2014 for failing to complete his job responsibilities

Applicant worked or Company B from April to November 2014 as an information security manager. SOR ¶ 1.b stems from this employment. The SOR alleges:

SOR ¶ 1.b: Alleges:

You were terminated from your employment at [Company B] in about November 2014 for failure to perform an audit on a computer used to process classified information as required by the NISPOM Section 8-602a. You completed a tracking log indicating you perform the audit on October 24, 2014, and when confronted about the audit, you continued to claim you had completed the audit. A subsequent investigation determined you did not complete the audit and were capable for falsifying business/government records and not acting in accordance with the [Company B] code of ethics.

In his Answer, Applicant denies SOR ¶ 1.b and sets forth several bases for his denial. First, Applicant states that he does not believe that he was "fired from his position." He bases this statement on the facts that he successfully collected unemployment as being "laid off," the employer did not protest his unemployment claim, and that he was not required to reimburse the company for his relocation funds as he would have been required to do if he had been terminated for cause.

In his Answer and testimony, Applicant further supports this position by referencing an email exchange he had with a former coworker wherein Applicant stated that he told a potential employer that he had been "downsized." In this same email, Applicant states

that his former manager and a human resources (HR) representative would not provide him with any information as to why he was "let go, just that [he] was." He characterizes a statement made by the former coworker in an email "no one is saying what happened." Applicant submitted an email exchange with HR wherein HR stated that it would not provide Applicant with a copy of the JPAS incident report (GX 5) concerning his termination or any documentation concerning why he was "dismissed," and that he did not need to complete any forms in order to apply for unemployment. (Tr. 34-35; AX N.) Applicant also noted during his testimony that he was offered another position with the employer in another state approximately three weeks after he was terminated. (Tr. 35.)

However, Applicant testified that in 2014:

> APPLICANT: I was -- same thing, human resources called me into their office and just said that I was terminated and that was it. I wasn't given any reason.
>
> ADMIN. JUDGE: So that was in November of 2014, you were --
>
> APPLICANT: Yes.
>
> ADMIN. JUDGE: -- they told you, you were fired?
>
> APPLICANT: Yes, ma'am.
>
> ADMIN. JUDGE: But you didn't put that on your security clearance application?
>
> APPLICANT: Well not fired, just terminated, and then I --
>
> ADMIN. JUDGE: Well what do you think terminated means?
>
> APPLICANT: I attempted to find out after, what the reason was.
>
> ADMIN. JUDGE: What do you think terminated means?
>
> APPLICANT: I don't know ma'am. It could mean anything. (Tr. 87-88.)

The second basis of Applicant's denial of SOR ¶ 1.b is that his "position did not include performing audits on computers. This was the responsibility of [a coworker]." (Answer.)

During his testimony, Applicant made the following assertions regarding performing audits:

1) It was not Applicant's job to perform NISPOM audits, and he did not have the necessary authorizations to do them. Performing NISPOM audits was the responsibility of his coworker. (Tr. 35-36.)

2) The audits were divided into the technical part and the policies and procedures part. It was Applicant's coworker's responsibility to perform the technical part of the audits and Applicant's responsibility to perform the policy and procedure part of the audits. (Tr. 62-63.)

3) Applicant never performed any of the audits. (Tr. 70.)

4) Applicant described audits in general as being about 90% policies and procedure and 10% technical. (Tr. 92.)

5) Applicant and his coworker performed as a team wherein Applicant performed the policy and procedure part of the audits and his coworker performed the technical part because Applicant did not have the required credentials to do so. (Tr. 128-129.)

The conduct alleged in SOR ¶ 1.b is based on a November 11, 2014, JPAS incident report (GX 5) and the employer's report of findings of an investigation dated November 20, 2014. The report of investigation states:

> The investigation determined that [Applicant] failed to perform an audit on a computer used to process classified information as required by the NISPOM section 8-602a. In addition, [Applicant] recorded an entry in the audit log book indicating that he did in fact complete the audit on October 24, 2014. Finally, [Applicant] was not truthful when confronted about this. This security incident was the result of an intentional disregard for the NISPOM requirements and of the [company's] Code of Ethics. The investigation deems [Applicant] culpable for an intentional security incident and as a result his employment with the company was terminated. (GX 4.)

The report lists the individuals involved in the investigation, one of whom is a contractor. The report sets forth details of conversations between Applicant and the contractor regarding Applicant's performance of an audit on classified computer #6, nicknamed "Poseidon." The report also includes an email exchange between Applicant and the contractor wherein Applicant represents that he performed the audit on October 24, 2014, but forgot to record an entry in the safe logbook.

The report also gives details of a meeting and conversation between Applicant and his supervisor. Applicant's supervisor, who was also the FSO, confronted Applicant about

routinely submitting inaccurate and incomplete reports and asked if Applicant had performed the required audit. Applicant again confirmed that he had.

The report then delineates the process of the investigation that unequivocally concluded that Applicant did not perform the required audit on the classified computer Poseidon on October 24, 2014, as he recorded in the logbook and represented in conversations, emails, and during a meeting.

Following the investigation, the HR manager and the ethics officer interviewed Applicant about the results of the investigation and Applicant again stated that he had completed the audit as required. Applicant was terminated for his conduct.

Applicant refutes the report of investigation on the following bases:

1) Applicant never met the contractor and does not know who he is;

2) Applicant confirmed that his email address was accurate, but stated he never exchanged emails with the contractor;

3) Applicant was out of state on vacation at the time of these incidents;

4) Applicant was never confronted by his supervisor about his job performance;

5) Applicant was never interviewed about the results of the investigation. (Tr. 37-39; Tr. 74-77.)

Applicant also testified that the report was inaccurate because classified computer #6 was not nicknamed Poseidon. According to Applicant, Poseidon was the name of a computer numerically controlled (CNC) machining tool on which audits were not only not required, but could not be performed. (Tr. 72-73.)

Applicant submitted a January 27, 2014, letter from DSS to the 2014 employer's FSO. Although prior to Applicant's employment, the letter states that DSS conducted a security vulnerability assessment at the facility and rated it "commendable." The assessment found six vulnerabilities, which are delineated in the letter. The fourth vulnerability, which was corrected on the spot, was: "Security relevant objects are not audited for failed access." It lists the systems effected, which includes "Poseidon." (AX T.)

Finally, during his testimony Applicant asserted, for the first time, that the events as described in the report could not have happened because he was visiting his daughter in another state on the specified dates. In support of this assertion, Applicant submitted by email attachment three copies of photographs of him with his daughter. (AX X – AX AA.)

Each photograph is attached to the email as a "JPG" file, which is "a computer file format for the compression and storage of digital images." (merriam-webster.com.) The photographs in the JPG files can be opened on a computer to view/print. The JPG file names appear as "10.26.14 Picture.jpg;" "10.30.14 Picture.JPG;" and "10.23.14 Picture.JPG." The email states that "each JPG can have the metadata shown by simply clicking on file info on the picture itself." The metadata includes the date, time, and location of where the picture was taken. (AX Y.) However, this type of metadata can be edited using widely available smartphone applications such as "pixelgarde" and "metapho." Applicant did not offer any other evidence to corroborate the dates his travel.

> Applicant failed to properly disclose the 2014 and 2016 employment terminations on a security clearance application and in two background interviews.

SOR ¶ 1.d: Alleges that when Applicant answered "no" on his e-QIP on November 1, 2016, "no" to Section 13C, which asks: in the last seven years, have you been "fired from a job" he falsified material facts by deliberately failing to disclose his terminations from two employers as set forth in SOR ¶¶ 1.a and 1.b.

Applicant denies this allegation in his Answer and states:

> I did not falsify information on the e-QIP. I do not believe I was terminated from this employer. If I was terminated I would have listed this on the e-QIP form. I did not deliberately fail to disclose anything.

It is unclear from Applicant's Answer whether he is referring to the 2014 or the 2016 employer. However, Applicant received a letter from his 2016 employer dated August 22, 2016, which stated that Applicant was terminated effective that same day. (AX K.)

Applicant also testified that he filed an ethics complaint with the 2016 employer to determine why he was terminated.

> DEPARTMENT COUNSEL: I don't see your ethics claim in here. Do we have a copy of your ethics claim?
>
> APPLICANT: No. I don't have a copy.
>
> DEPARTMENT COUNSEL: What was in it to your best recollection? What did you allege? What was the concern?
>
> APPLICANT: I wanted to know why I was fired, why they sent me home, basically just to really find out what happened and then I received that letter.

In a November 24, 2014, email to HR, Applicant stated "I have a right to know what information was submitted into JPAS on my clearance especially since it was

recommended that my accesses be revoked." When queried by Department Counsel why he did not disclose the JPAS incident report on his e-QIP, Applicant stated that he did not know what information was in the incident report and that "anything can be entered in JPAS for any reason."

SOR ¶ 1.e: Alleges that Applicant falsified material facts during a personal subject interview (PSI) on January 25, 2018, when he stated that he did not know the reason for his termination from the 2016 employer.

In his Answer, Applicant denies this allegation and contends that he did not know the reason for his "termination." He testified that he did not find out the reason for his termination until he received the Government's discovery in December 2018. (Tr. 49.)

SOR ¶ 1.f: Alleges that Applicant falsified material facts during a PSI on November 2, 2017, when he stated that he was laid off from his 2014 employment, but was in fact deliberately concealing that he had been terminated.

In his Answer, Applicant denies this allegation and states:

> I was laid off from this employer and filed and collected unemployment for being laid off. The information contained in the SOR is false. I also made attempts to obtain the reason why I was let go from HR and other employees and was given no information at all.

In his 2017 PSI, Applicant told the investigator that he was laid off for unknown reasons with about 30 other people. (GX 2.) In an email exchange asking a coworker to be a reference, Applicant stated that he had told a potential employer that he had been "downsized" because HR and Applicant's supervisor would not provide him with "any information as to why I was let go, just that I was." (AX N.) On his 2016 e-QIP, Applicant listed the reason for leaving his 2014 employer as "unknown. Reason for termination was never provided by employer. Unemployment claim was not contested. Reason given by employer to [another state] unemployment office was I was laid off due to lack of work." (GX 1.)

As set forth above under SOR ¶ 1.b, Applicant was called into the HR office and told he was terminated.

SOR ¶ 1.g: Alleges that Applicant falsified material facts on a resume that he submitted for employment in October 2016 when he reported that he obtained a bachelor's degree from [a university] in August 2011 with a 3.8 GPA.

Applicant submitted the resume for employment with Company C, where he worked from to October 2016 until October 2017 as an information systems security and technology manager. In his Answer, Applicant admits in part and denies in part SOR ¶ 1.g. Applicant admits that he did not graduate from the university, and did not take any classes there. He states that he enrolled with the intent of attending, and August 2011

would have been his projected graduation date. He further states that he received the 3.8 GPA after transferring credits from "prior training and military service" to the university. Applicant also stated that it was not his "intent to defraud or make a false claim of having a bachelor's degree."

Applicant also attached with his Answer a biography. The document is undated, however, he describes work experience through October 2017. Applicant states in the document that he dropped out of high school and then received a GED in August 2002. There is no reference to any attendance of or enrollment in any college or university. (AX A.)

In his January 2018 PSI, Applicant confirmed that he had not graduated with any college degrees or taken any college classes within the last 10 years. When confronted about the resume he submitted that stated that Applicant had graduated from [a university] with a bachelor's degree in August 2011. Applicant stated that he did not take any classes at the university, but that he did accumulate college credits for his military training and work experience. (GX 2.)

In his August 2018 responses to the Government's interrogatories, specifically when asked to provide copies of all college transcripts and diplomas for all completed degrees, Applicant responded "I do not possess any college transcripts or diplomas. I have no completed degrees. I only have a GED." (GX 3.)

However, Applicant also reported on his 2016 resume that he was enrolled in a university in a dual Master of Science in Cybersecurity with a 4.0 GPA and a Bachelor of Science in Information Technology with a 4.0 GPA with an anticipated graduation date of April 2019. (GX 6.) He testified that the university was primarily on-line and that he had completed approximately 18 courses. He further testified that he was in the process of transferring his credits from this university and another (not previously mentioned) college where he had gotten credits for his military training to another on-line university starting in August 2019. He hoped to complete his degree by December 2019. (Tr. 110; Tr. 134-136.)

Applicant completed a talent profile as part of his job application for the employer to whom he submitted his 2016 resume. (AX H.) Under the education section, he did not list the false information regarding his 2011 bachelor's degree and 3.8 GPA. However, he listed the university with the dual master's and bachelor's programs and stated that he had been attending that university from January 2016 until the present. (GX 6.)

When asked by Department Counsel why he provided this false information on his 2016 resume, Applicant responded:

> APPLICANT: I had placed it on my resume years ago and it had a graduation date I think of 2011, and 24 then it was just -- it stayed on my resume.

DEPARTMENT COUNSEL: Now why'd you put a graduation date in for a program that you never took a class in?

APPLICANT: No I don't mean a graduation -- I mean like a projected graduation date. (Tr. 58-59.)

Applicant also offered testimony as to why his 2016 resume contained false information:

I remember enrolling in [the university] back in 2008, I transferred all the credits I had there, which is where the GPA had come from. I had placed it on an older version of my resume with the graduation date of 2011 and then I hadn't taken it off my resume. (Tr. 114.)

SOR ¶ 1.h: Alleges that Applicant falsified material facts on a resume he submitted for employment with [Company B] in April 2014 when he reported that he obtained a bachelor's degree from [a university] with a GPA of 3.8.

The 2014 resume listed the city and state where the university was located, the 2016 resume did not. The 2016 resume included a "completion" date of August 2011, the 2014 resume did not. Additionally, the font and formatting are different on the 2014 and 2016 resumes.

In his Answer, Applicant's response to this allegation is the same as his response to SOR ¶ 1.g.

Applicant has failed to resolve the outstanding balance on his Company B travel credit card

SOR ¶ 1.c: Alleges that Applicant failed to pay a collection account of $1,528 on a credit card issued by Company B in about October 2014, and that the account remains delinquent.

The debt is verified by a 2018 credit report, Applicant's statements during his November 2017 PSI, and his testimony. According to Applicant, the balance owed is for expenses for his out-of-state travel for training in November 2014 and should have been paid by his employer. In his responses to interrogatories, Applicant states that the account was paid. He testified that he submitted his expense report to HR prior to his termination on November 17, 2014. He further testified that he has done online disputes of this debt multiple times. He also stated that he has written multiple letters, faxed letters, and contacted various branches of the financial Institute that issued the credit card and there is no record of his name or Social Security number in their systems. (Tr. 44-46.) Applicant did not submit any copies of these dispute letters into the record.

On November 18, 2014, Applicant was provided with a form from HR via email to submit his expense report and receipts. On November 20, 2014, Applicant responded to

HR stating that HR should receive the expense report by the following week. (AX N.) Applicant did not submit a copy of the completed expense report into the record.

On August 20, 2018, Applicant submitted an online dispute with the stated reason, "I have never paid this account late. My account balance is incorrect." (AX P.) In his Answer, Applicant stated that the credit-card company will not accept any payments on his behalf. He further stated that he has never been successful in disputing this account or having it removed from his credit reports but does not believe he owes the money for this card. Applicant testified that the account has been removed by one of the three major credit reporting agencies. (Tr. 44.) He did not provide any additional documentation regarding this account. This account remains unresolved.

Applicant's Character Evidence

Applicant submitted 13 letters of recommendation from: his current security manager supervisor, direct supervisor, FSO, five coworkers, and the IT director of the company where Applicant has worked as a consultant since 2016; and his former supervisor, platoon leader, and two coworkers. Collectively, the letters state that Applicant is a highly professional and trustworthy individual and recommend him for a security clearance. Additionally, 12 of the letters state that Applicant "is always very respectful of privacy, classified information, laws, rules, and regulations." (AX R.)

While on active duty, Applicant received numerous medals and awards. He achieved or exceeded course standards in his service school academic evaluations. (AX B.) Between 2014 and 2017, he completed multiple cybersecurity certifications. (AX G.) Applicant received a positive work performance evaluation from his employer in January 2017, wherein his supervisor stated that, Applicant "has taken a leadership role in documenting new procedures to ensure compliance with new regulatory requirements" while quickly assuming "all duties of the information systems security manager and alternate facility security officer with no difficulties."

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, *Safeguarding Classified Information within Industry* § 2 (Feb. 20, 1960), as amended.

Eligibility for a security clearance is predicated upon the applicant's meeting the criteria contained in the AG. 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 all available and reliable information about the person, past and present, favorable and unfavorable.

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." *See* 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. *See Egan*, 484 U.S. at 531. "Substantial evidence" is "more than a scintilla but less than a preponderance." *See v. Washington Metro. Area Transit Auth.*, 36 F.3d 375, 380 (4th Cir. 1994). The guidelines presume a nexus or rational connection between proven conduct under any of the criteria listed therein and an applicant's security suitability. *See* ISCR Case No. 92-1106 at 3, 1993 WL 545051 at *3 (App. Bd. Oct. 7, 1993).

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* 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 ¶ 2(b).

Analysis

Guideline E, Personal Conduct

The concern under this guideline is set forth in AG ¶ 15:

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. The following will normally result in an unfavorable national security eligibility determination, security clearance action, or cancellation of further processing for national security eligibility:

> (a) refusal, or failure without reasonable cause, to undergo or cooperate with security processing, including but not limited to meeting with a security investigator for subject interview, completing security forms or releases, cooperation with medical or psychological evaluation, or polygraph examination, if authorized and required; and
>
> (b) refusal to provide full, frank, and truthful answers to lawful questions of investigators, security officials, or other official representatives in connection with a personnel security or trustworthiness determination.

The Government has established by substantial evidence its *prima facie* case. The following disqualifying conditions apply:

> AG ¶16(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;
>
> AG ¶16(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;
>
> AG ¶ 16(c): credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any other single guideline, but which, when considered as a whole, supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the individual may not properly safeguard classified or sensitive information; and if
>
> 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, consideration of:

> (2) any disruptive, violent, or other inappropriate behavior; and
>
> (3) a pattern of dishonesty or rule violations.

The following mitigating conditions are potentially applicable:

AG ¶ 17(a): the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts; and

AG ¶ 17(c): the offense is so minor, or so much time has passed, or the behavior is so infrequent, or it happened under such unique circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment.

The Government's evidence establishes its *prima facie* case. Specifically, the January 2017 letter from Company A to DSS delineating the findings of investigation into Applicant's conduct combined with the 2016 JPAS entry are sufficient to show that Applicant was culpable of labor mischarging and failing to perform his assigned duties and was terminated as a result. The 2014 report of investigation combined with the 2014 JPAS entry are sufficient to show that Applicant failed to perform his assigned duties, falsely represented that he had performed such duties, both in a tracking log and when confronted, and was terminated as a result. This evidence, and the overall record evidence, establish that Applicant made false statements and representations during his PSIs and on his e-QIP.

The 2014 and 2016 resumes and 2016 job application contain information about Applicant's educational credentials that Applicant admits is false. The 2018 CBR and overall record evidence show that Applicant is individually liable for the $1,528 delinquent credit-card account and that the account remains unresolved.

Applicant continues to deny that he was culpable of the conduct that resulted in his 2016 termination. He supported this position by submitting the letter from the former FSO that refutes the January 2017 letter containing the results of the employer's investigation. The January 2017 letter states that the employer's investigation was based on badging data, video evidence, network login data, and cell phone records. The former FSO states that this cannot be accurate because Applicant worked in a classified area where there was no video surveillance, badged entry, or network login, and that it would not have been possible for the employer to obtain Applicant's personal cell phone records. The FSO also states that following Applicant's termination, she prepared for a DSS audit and found all software patches were completed and audits performed.

I find the letter from the former FSO to be unpersuasive. The former FSO was not a party to the investigation and was not present when any of Applicant's alleged conduct occurred. The January 2017 letter does not specify the locations from which badging data, video evidence, and login data were collected nor does it specify what cell phone records were collected. Applicant testified that a badge reader was installed on an external door shortly before he was terminated and that he routinely logged in to a network to use email. The January 2017 letter indicates that after discovering that Applicant had failed to conduct required NISPOM audits, the employer completed all auditing and software updates to ensure that no classified information had been compromised. This was part of the investigation into Applicant's conduct and was performed prior to the conclusion of the investigation. Further, the FSO has not worked for the employer since January 2019. It is unclear under what circumstances she left, what her relationship with her former employer is, and whether she has any bias toward Applicant or against her former employer.

In order to find that Applicant has met his burden of persuasion required to mitigate the Government's security concerns, I would have to find the following to be true:

In 2014 and 2016, employees in supervisory positions at two disparate companies separately conspired to create false records of investigation that contained derogatory information about Applicant, the two unrelated investigations each independently determined that Applicant had failed to perform audits as required by NISPOM, the FSOs from both companies entered false derogatory information about Applicant into JPAS, and the FSO of the 2016 employer reported false information about Applicant to DSS;

> The 2014 report of investigation was completely fabricated to include false copies of emails, as well as recitations of conversations that never occurred and meetings that never took place;
>
> The January 2014 DSS report of its audit contains erroneous information and that same erroneous information is in the 2014 employer's investigation;
>
> The conclusions of the investigation set forth in the January 2017 letter from Applicant's 2016 employer's FSO to DSS were completely false;
>
> Applicant's 2014 employment did not require him perform any audits;
>
> The false information about Applicant's 2011 bachelor's degree that appears on his 2016 resume in a different format and font and lists additional information from the false information on his 2014 resume is because Applicant simply failed to remove the false information from the 2014 resume when he created the 2016 resume;

> It was not Applicant's intention to defraud or make a false claim when he listed the false information about his education on two resumes and a job application;
>
> Applicant received a 3.8 GPA after transferring credits earned for prior training and military service, has completed approximately 18 courses in a dual master's and bachelor's degree program, but does not have any transcripts showing his earned credit hours;
>
> Applicant did not know that he was terminated from his 2014 and 2016 employers prior to completing his 2016 e-QIP, undergoing his 2017 and 2018 PSIs, and completing his employment history on his 2016 job application;
>
> Applicant properly submitted his expense report before he was terminated in November 2016 and has made extensive efforts to dispute the $1,528 collection account.

In light of all the record evidence, I do not believe the above statements to be true. Applicant's testimony and other record statements are replete with inconsistencies, omissions, and falsifications. He is not a credible, reliable, or trustworthy source. For example, Applicant repeatedly stated that his 2014 employment did not require that he perform audits. He then testified that, in fact, he performed the procedures and policies part of the audits, which constituted approximately 90% of the audits.

Further, Applicant cannot keep his stories straight about his education. He did not offer any plausible explanation for why he falsified his 2014 and 2016 resumes or his 2016 job application. He testified that he had listed false information on his 2014 resume and just "hadn't taken it off" his 2016 resume. Yet, the font and formatting, and the information itself differs between the two resumes. In his January 2018 PSI, Applicant confirmed that he had not taken any college classes within the last 10 years, but he listed on his 2016 job application that he had been enrolled in a dual master's and bachelor's degree program since January 2016. He testified that he has taken approximately 18 courses in the dual degree program, has received college credits for his military training and work experience from another college – not the one listed on his resumes – and is in the process of transferring all his credits to yet another university, but does not have any transcripts.

An act of falsification has security significance independent of the underlying conduct. *See* ISCR Case No. 01-19278 at 7-8 (App. Bd. Apr. 22, 2003). The mitigation of the underlying conduct has little bearing on the security significance of the falsification, particularly where there are multiple falsifications. ISCR Case No. 08-11944 at 3 (App. Bd. Aug 15, 2011). Previous inconsistent statements may be considered in assessing an applicant's credibility, evaluating evidence, and considering whether the applicant has demonstrated rehabilitation, even though they were not alleged in the SOR. ISCR Case No. 08-09232 at 3 (App. Bd. Sep. 9, 2010.)

Applicant's ongoing equivocations about the definition of "terminated," about whether he was terminated or laid off, about his knowledge that the 2014 JPAS entry contained derogatory information, and about his educational background demonstrate that he does not accept responsibility for his conduct.

Applicant continues to assert that he did not do what the 2014 and 2016 investigations state he did. He defends this position that he was not fired for cause by showing that he successfully collected unemployment benefits from the 2014 and 2016 employers. He also notes that the 2014 employer offered him another position after his termination.

However, Applicant has not pursued any avenue against either employer for wrongful termination. Even if Applicant did not actually know the specific reasons for the terminations until he received the Government's evidence, it does not explain why, if he did nothing wrong, he failed to take any action to be reinstated or otherwise compensated. This is particularly perplexing given that he has pictures which he asserts exonerate him of the accused wrongdoing that resulted in his 2014 termination.

I do not find Applicant's version of events to be plausible. The 2014 and 2016 investigations are not elaborate schemes created for the purpose of terminating Applicant. He failed to properly perform his job duties and got caught. I am also not convinced that Applicant did not alter the dates on the photographs he submitted.

Further, regardless of whether or not Applicant was specifically informed by his employers of the reasons he was terminated in 2014 and 2016, he had an obligation to be candid and forthcoming on his e-QIP and during his two PSIs. He was aware of the 2014 JPAS entry, as evidenced by his email to HR expressing concern over the negative impact that the entry could have on his security clearance. He should have disclosed his knowledge of the JPAS entry to the investigators during his PSIs and his failure to do so raises security concerns.

Applicant has worked in cybersecurity and as an FSO and has held a security clearance since 2008. It is simply not plausible that Applicant did not understand that he was required to be forthcoming about derogatory or security-relevant information of which he was aware during his background investigation and the adjudication of his security clearance. His ongoing failure to accept responsibility for his actions, including his deliberate falsifications and omissions, and his overall lack of credibility, raise significant concerns about his ability to protect classified information. He has not met his burden of persuasion.

I find that Applicant intentionally falsified material facts on his e-QIP, during his PSIs, and to his employers. His 2014 and 2016 terminations were the result of his failure to comply with security requirements and ethical standards. He has failed to resolve a delinquent account for which he is personally liable. None of the mitigating conditions apply.

Guideline M, Use of Information Technology

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.

While Applicant's failure to conduct audits as required by NISPOM falls under the general concern of Guideline M, none of the disqualifying conditions specifically apply. Applicant's disqualifying conduct is more appropriately analyzed under Guideline E, as set forth above.

Whole-Person Concept

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. In applying the whole-person concept, an 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. An 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.

I have incorporated my comments under Guidelines E and M in my whole-person analysis. Some of the factors in AG ¶ 2(d) were addressed under those guidelines, but I have also considered the following:

Applicant has made intentionally false and misleading statements and omissions throughout the security clearance process, and continues to equivocate about his conduct. His ongoing lack of consistency and clarity in recounting the details of his conduct and his failure to accept responsibility for his behavior remain concerns.

After weighing the applicable disqualifying and mitigating conditions under Guidelines E and M, and evaluating all the evidence in the context of the whole person, I

conclude Applicant has not mitigated the security concerns raised by his personal conduct. Accordingly, I conclude he has not carried his burden of showing that it is clearly consistent with the national interest to grant him eligibility for access to classified information.

Formal Findings

As required by section E3.1.25 of Enclosure 3 of the Directive, I make the following formal findings on the allegations in the SOR:

Paragraph 1, Guideline E (Personal Conduct):	AGAINST APPLICANT
Subparagraphs 1.a - h:	Against Applicant
Paragraph 2, Guideline M (Use of Information Technology):	FOR APPLICANT
Subparagraph 1.a:	For Applicant

Conclusion

I conclude that it is not clearly consistent with the national interest to grant Applicant's eligibility for a security clearance. Eligibility for access to classified information is denied.

Stephanie C. Hess
Administrative Judge