**DEPARTMENT OF DEFENSE**
**DEFENSE OFFICE OF HEARINGS AND APPEALS**

| | | |
|---|---|---|
| In the matter of: | ) | |
| | ) | |
| | ) | ISCR Case No. 15-06751 |
| | ) | |
| Applicant for Security Clearance | ) | |

## Appearances

For Government: Rhett E. Petcher, Esq., Department Counsel
For Applicant: Troy L. Nussbaum, Esq.

02/08/2018

## Decision

LOUGHRAN, Edward W., Administrative Judge:

Applicant did not mitigate the personal conduct security concerns. Eligibility for access to classified information is denied.

## Statement of the Case

On November 17, 2016, the Department of Defense (DOD) issued a Statement of Reasons (SOR) to Applicant detailing security concerns under Guideline E, personal conduct. Applicant responded to the SOR on February 2, 2017, and requested a hearing before an administrative judge.

The case was assigned to me on August 16, 2017. The Defense Office of Hearings and Appeals (DOHA) issued a notice of hearing on August 29, 2017, scheduling the hearing for September 20, 2017. The hearing was convened as scheduled. DOHA received the hearing transcript (Tr.) on September 28, 2017.

## Procedural and Evidentiary Rulings

### Motion to Amend SOR

Department Counsel moved to amend SOR ¶ 2.b by deleting the words "or delete" from the allegation. The motion was granted without objection.

Applicant's objection to Department Counsel's motion to amend SOR ¶ 2.d was overruled. The allegation now reads:

> You gave false answers in response to interrogatories provided to you by the Defense Office of Hearings and Appeals on or around August 5, 2016. In providing additional information regarding your July 10, 2015 subject interview, you stated that the computers at issue were running a version of "Unreal Tournament," an online first-person shooter game. In fact, you knew that the computers were being used as a warez server in addition to being used to run Unreal Tournament.

### Evidence

Government Exhibits (GE) 1 and 2 were admitted in evidence without objection. GE 3 was admitted over Applicant's objection. Applicant testified, called three witnesses, and submitted Applicant's Exhibits (AE) A through J and AA through JJ. AE A through J and BB through JJ were admitted without objection. AE AA is a memorandum from Applicant's attorney commenting on the reliability of GE 3. The objection to AE AA as substantive evidence was sustained. However, it will be considered as argument.

## Findings of Fact

Applicant is a 47-year-old network engineer employed by a defense contractor since 2012. He has a bachelor's degree. He is married for the third time. He has four children and two stepchildren.[1]

Applicant worked as a field technician for an Internet services provider from the late 1990s to the early 2000s. His responsibilities included maintaining the hardware. Applicant stated that he had no software responsibilities. At some point in the late 1990s, he told one of the owners that in the past he downloaded software using warez,[2] an online site that permitted pirated software to be downloaded and shared. The owner told him that it was a bad idea, and that he was not to do it at the company.[3]

[1] Tr. at 28, 31.

[2] Warez is a common computing and broader cultural term referring to pirated software (i.e. illegally copied, often after deactivation of anti-piracy measures) that is distributed via the Internet. *See* https://en.wikipedia.org/wiki/Warez.

[3] Tr. at 29-39, 104-134; Applicant's response to SOR; AE B.

The company decided to offer the online game Unreal Tournament to their customers as an added feature. A server was sent to Applicant's home to be used for the online game, which he transported to the company. At some point, before or after the server was shipped to Applicant, warez software was installed on the server that permitted pirated software to be downloaded and shared. Applicant used the warez on the server to download software, including educational material, music, games, pornographic[4] videos, and movies. Applicant estimated that he had several dozen CDs and DVDs of pirated software at his home.[5]

The FBI was conducting an investigation into pirated software and went to Applicant's home in December 2001. Applicant's wife called him and told him they were there. He told her to hide the pirated software. Applicant was interviewed by the FBI on several occasions. He did not provide a signed statement, but the interviews were summarized by the FBI agents. The report of the interviews indicated that Applicant initially emphasized that the only purpose of the server was to be a gaming server, but he subsequently stated that the true purpose of the server was for servicing pirated software or warez. Applicant stated that his participation began when a co-worker (AB) requested that Applicant allow for the placement of the warez server on the company's network. In exchange for his cooperation, Applicant was given "leech" privileges to access all the files on the network. The report also noted that Applicant stated that in response to a higher-than-anticipated traffic volume that threatened to crash the current server, another warez server with extremely high storage capacity was shipped to him. This server was collocated with the original gaming server.[6]

Applicant gave the FBI his pirated software, and he provided the FBI agents with consent to search his home. Computers, pirated software contained on CDs and DVDs, and other items were seized. The FBI also seized legitimate non-pirated CDs and DVDs, including unopened Christmas presents.[7]

Applicant retained an attorney and about a month later was interviewed by the FBI at the U.S. Attorney's Office pursuant to a proffer agreement. The FBI report of this interview is somewhat different than the report of the initial interview, but for the most part, consistent with Applicant's hearing testimony. He stated that he was unaware that the server was being used as a warez server until he learned it from AB a couple of weeks after receiving the server. Applicant cooperated with the FBI, acted as a confidential informant for two to three years, and wore a wire. No charges were ever filed against him, nor were any charges ever filed against AB. The FBI retained the CDs and DVDs, legitimate and pirated, but returned other seized items to Applicant.[8]

[4] I am using the common definition of pornography, as opposed to its legal definition.

[5] Tr. at 34-43, 78-80; Applicant's response to SOR; AE B.

[6] Tr. at 41, 48, 76-77; Applicant's response to SOR; AE G.

[7] Tr. at 43-47, 53-54; Applicant's response to SOR; AE D, E.

[8] Tr. at 49-54, 139-153; AE D, E.

Applicant was interviewed for his background investigation in July 2015. A signed statement was not obtained, but the interview was summarized in a report of investigation (ROI). Applicant responded affirmatively to a question whether he had ever been investigated by a law enforcement agency for pirating software or media, or for aiding anyone else to do so. He described being investigated by the FBI, as follows:

> Without Subject's knowledge, a warez server was installed on a server that was under Subject's area of responsibility. The warez sever program is illegal software used to distribute copyrighted or pirated software and files, such as movies and music. As the systems administrator, Subject would regularly receive Digital Millennium Copyright Act (DMCA) notifications that users were illegally downloading software, movies, and music. As a result of these notifications, Subject was responsible for shutting down internet access to those customers that DMCA notices were directed against. During the FBI Operation Buccaneer, the FBI investigated, arrested, and charged individuals involved in warez servers. One day in the mid to late 1990's, exact date unrecalled, special agents from the FBI arrived at Subject's job location in [location] and confiscated the server with the warez program on it and Subject's computer. On Subject's work computer was the account and billing information for the customers of [Applicant's employer]. Subject was then questioned concerning his knowledge of the warez server and the customer account information on his work computer. Subject was an authorized user for the customer account information. Subject denied that he had any knowledge of the warez server installed on the servers in [location]. As a result of the FBI's investigation, Subject was never arrested, charged, or convicted of any offense. Subject has not received any additional notifications concerning his involvement or knowledge of the warez server.

DOHA issued interrogatories to Applicant on August 5, 2016. He responded on an indeterminate date. Subject to the following corrections and additional information, he certified the ROI as accurately reflecting his interview:

> After personal reflection the year was either late 2000 or early 2001, the exact day and month cannot be recalled.
>
> The FBI's Operation Buccaneer was a national investigation by the FBI's cybercrimes division for Illegal Software and conducted nationally at different locations. The server in question was being monitored and tracked by the FBI, it was shipped to my home address from another authorized [Applicant's employer] Employee whom had permission from the company to place it in service in the [location] facility. All company hardware at that time, under employment with [Applicant's employer] was shipped to my home address for placement in remote locations. The server was running a game server called "Unreal Tournament" by GT Interactive, Atari Inc. This is how it fell under my realm of duties, as an administrator. It was authorized to be installed by [Applicant's employer]

> as an added-value-service to current customers who liked to play on-line games. During this investigation the FBI seized not only company property but also personal property. In which all of my own personal property was returned by the FBI after examination. As a result of the FBI's investigation I was never charged with any crime.

Applicant denied intentionally providing false or misleading information during the background interview and in response to DOHA interrogatories. He testified that the part of the interview about the incident only lasted about 20 to 30 minutes. He stated that he told the investigator that when he racked the server up, he was unaware that warez was installed on it. He stated that he eventually became aware that the server was being used as a warez server, but "installed" is a term of art, meaning placing the software on the server. Therefore, his statement to the investigator was correct, that he had no knowledge of how the warez software was "installed" on the server. He stated that he did not correct the ROI in the interrogatories, because the ROI was accurate. He also stated that he was advised not to volunteer information. He stated that in retrospect, he should have also volunteered that he downloaded pirated software. He stated that he has not downloaded or otherwise used any pirated matter since the FBI investigation, and he has been completely honest with his employers about his involvement in the incident.[9]

Applicant called witnesses and submitted documents and letters attesting to his excellent job performance. He is praised for his trustworthiness, work ethic, reliability, loyalty, patriotism, leadership, dedication, maturity, judgment, candor, expertise, professionalism, honesty, responsibility, commitment, and integrity. He is recommended for a security clearance.[10]

## Policies

This case is adjudicated under Executive Order (EO) 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; DOD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the adjudicative guidelines (AG), which became effective on June 8, 2017.

When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the adjudicative guidelines. In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially disqualifying conditions and mitigating conditions, which are to be used in evaluating an applicant's eligibility for access to classified information.

These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, administrative judges apply the guidelines in

[9] Tr. at 54-74, 87-92, 98, 156-164; Applicant's response to SOR; AE F.

[10] Tr. at 101-137, 155-164; AE B, C, H-J.

conjunction with the factors listed in the adjudicative process. The administrative judge's overarching adjudicative goal is a fair, impartial, and commonsense decision. According to AG ¶ 2(a), the entire process is a conscientious scrutiny of a number of variables known as the "whole-person concept." The administrative judge must consider all available, reliable information about the person, past and present, favorable and unfavorable, in making a decision.

The protection of the national security is the paramount consideration. AG ¶ 2(b) requires that "[a]ny doubt concerning personnel being considered for national security eligibility will be resolved in favor of the national security."

Under Directive ¶ E3.1.14, the Government must present evidence to establish controverted facts alleged in the SOR. Under Directive ¶ E3.1.15, the applicant is responsible for presenting "witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by the applicant or proven by Department Counsel." The applicant has the ultimate burden of persuasion to obtain a favorable security decision.

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

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

## Analysis

### Guideline E, Personal Conduct

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

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

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

(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;

(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

(e) personal conduct, or concealment of information about one's conduct, that creates a vulnerability to exploitation, manipulation, or duress by a foreign intelligence entity or other individual or group. Such conduct includes:

(1) engaging in activities which, if known, could affect the person's personal, professional, or community standing.

Applicant used the warez on his company's server to download pirated software, including educational material, music, games, pornographic videos, and movies. When the FBI went to his home, he told his wife to hide his pirated software. Those actions reflect questionable judgment and an unwillingness to comply with rules and regulations. They also created vulnerability to exploitation, manipulation, and duress. AG ¶¶ 16(c) and 16(e) are applicable.

Much of the information provided by Applicant during his background interview and in his response to interrogatories was true. It was the omitted information that was misleading. Nowhere in the interview or his clarifying comments in the interrogatories does he admit any culpability in the incident. I did not find Applicant's explanation for the background interview and his response to DOHA interrogatories to be credible. While there is some question when Applicant became aware the server was being used as a warez server, he clearly knew it before the FBI investigation and used the server to download pirated material. I find that his omission of that information was intentional and done to mislead the government about his participation in the matter. His false statement in response to interrogatories that "all of [his] own personal property was returned by the FBI after examination" is consistent with that intent, because it does not reveal that the FBI retained his pirated software. AG ¶ 16(b) is applicable.

AG ¶ 17 provides conditions that could mitigate security concerns. 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;

(b) the refusal or failure to cooperate, omission, or concealment was caused or significantly contributed to by advice of legal counsel or of a person with professional responsibilities for advising or instructing the individual specifically concerning security processes. Upon being made aware of the requirement to cooperate or provide the information, the individual cooperated fully and truthfully;

(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.

Applicant's conduct at his former company and with the FBI occurred more than 16 years ago. He cooperated with the FBI, acted as a confidential informant for two to three years, and wore a wire. There is no evidence that he has downloaded or otherwise used any pirated matter since the FBI investigation. That conduct, as alleged in SOR ¶¶ 1.a and 1.b, is mitigated.

Having determined that Applicant intentionally omitted information in an attempt to mislead the government, I have also determined that his explanations that the omissions were unintentional were also false. It would be inconsistent to find that conduct mitigated.[11]

[11] *See* ISCR Case 03-22819 at 4 (App. Bd. Mar. 20, 2006), in which the Appeal Board reversed the Administrative Judge's decision to grant Applicant's security clearance:

> Once the Administrative Judge found that Applicant deliberately falsified a security clearance application in September 2002, the Judge could not render a favorable security clearance decision without articulating a rational basis for why it would be clearly consistent with the national interest to grant or continue a security clearance for Applicant despite the falsification. Here, the Judge gives reasons as to why he considers the falsification mitigated under a "whole person" analysis, namely that Applicant has matured, has held a position of responsibility, recognizes how important it is to be candid in relation to matters relating to her security clearance, and has changed her behavior so that there is little likelihood of recurrence. However, the Judge's conclusion runs contrary to the Judge's rejection of Applicant's explanations for the security clearance application falsification. At the hearing (after earlier admitting the falsification in her March 2003 written statement to a security investigator), Applicant testified that she had not

## 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):

> (1) the nature, extent, and seriousness of the conduct; (2) the circumstances surrounding the conduct, to include knowledgeable participation; (3) the frequency and recency of the conduct; (4) the individual's age and maturity at the time of the conduct; (5) the extent to which participation is voluntary; (6) the presence or absence of rehabilitation and other permanent behavioral changes; (7) the motivation for the conduct; (8) the potential for pressure, coercion, exploitation, or duress; and (9) the likelihood of continuation or recurrence.

Under AG ¶ 2(c), the ultimate determination of whether to grant eligibility for a security clearance must be an overall commonsense judgment based upon careful consideration of the guidelines and the whole-person concept.

I considered the potentially disqualifying and mitigating conditions in light of all the facts and circumstances surrounding this case. I have incorporated my comments under Guideline E in my whole-person analysis. I considered Applicant's favorable character evidence. His actions with the warez server and telling his wife to hide the pirated software occurred more than 16 years ago. He cooperated with the FBI, acted as a confidential informant for two to three years, and wore a wire. Those actions mitigate that conduct. However, his intentionally misleading information about his conduct is not mitigated.

The record evidence leaves me with questions and doubts as to Applicant's eligibility and suitability for a security clearance. I conclude Applicant did not mitigate the personal conduct security concerns.

## Formal Findings

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

| | |
|---|---|
| Paragraph 1, Guideline E: | Against Applicant |
| Subparagraphs 1.a-1.b: | For Applicant |
| Subparagraphs 1.c-1.d: | Against Applicant |

---

intentionally falsified her application. Given the Judge's rejection of this explanation as not being credible, it follows that the Judge could not have concluded Applicant now recognizes the importance of candor and has changed her behavior.

## Conclusion

It is not clearly consistent with the national interest to grant Applicant eligibility for a security clearance. Eligibility for access to classified information is denied.

_____
Edward W. Loughran
Administrative Judge