



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



In the matter of:)
)
) ISCR Case No. 23-00919
)
 Applicant for Security Clearance)

Appearances

For Government: Mark D. Lawton, Esq., Department Counsel
For Applicant: *Pro se*

02/15/2025

Decision

HALE, Charles C., Administrative Judge:

This case involves security concerns raised under Guideline F (Financial Considerations), Guideline M (Use of Information Technology), and Guideline J (Criminal Conduct). Eligibility for access to classified information is denied.

Statement of the Case

Applicant submitted a security clearance application on May 12, 2022. On August 8, 2023, the Department of Defense (DoD) sent him a Statement of Reasons (SOR) alleging security concerns under Guidelines F, M, and J. The DoD 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 adjudicative guidelines (AG) promulgated in Security Executive Agent Directive 4, *National Security Adjudicative Guidelines* (December 10, 2016).

Applicant answered the SOR on August 28, 2023, and requested a decision on the written record without a hearing. Department Counsel submitted the Government's

written case on November 7, 2023. On November 7, 2023, a complete copy of the file of relevant material (FORM) was sent to Applicant, who was given an opportunity to file objections and submit material to refute, extenuate, or mitigate the Government's evidence. He received the FORM on November 17, 2023, and submitted a Response on November 19, 2023, along with the IRS 1040 forms for tax years 2013-2018, which will be collectively identified as Applicant Exhibit (AE) A.

The SOR and the Answer are the pleadings in the case. FORM Items 2 through 4 and AE A are admitted into evidence without objection.

Findings of Fact

In Applicant's Answer to the SOR, he admitted all of the allegations in the SOR. His admissions are incorporated in my findings of fact.

Applicant is a 37-year-old male. He holds a Ph.D. earned in 2020 while living overseas. He earned his master's degree in 2012 and his bachelor's degree in 2010 from the same U.S. university. He has worked for a DoD contractor since May 2022. He is single and has no children. The evidence concerning his taxes and use of information technology is summarized below.

Guideline F

SOR ¶ 1.a: failed to file as required Federal income tax returns for tax years 2013 through 2018. Applicant admits the allegation. As mitigation he offers that he was living overseas in a country where he believed there was a treaty that income earned in the one country would only be taxed by the country where he was residing but not both. He notes the IRS had not reached out to him, so he concluded it was "likely" not an issue for them. (Answer.) His Federal tax account transcripts for the tax years alleged reflect no tax returns filed for the years provided. (Item 3.) In his Response, he again acknowledged not filing his tax returns for tax years 2013-2018 and attached the unfiled 1040 forms with calculations that indicated he owed no money. He stated had he thought he owed money or had he been living in the United States he would have "definitely" filed his Federal returns. He offers as mitigation these incidents happened several years ago while living and working on his Ph.D. overseas, and since returning to the United States, he has started working with a tax preparer to file returns for the missing years. In his Response, he notes as mitigation he filed his tax returns for tax years 2019 through 2022.

Guideline M

SOR ¶ 2.a: Applicant illegally downloaded movies from his school computer while attending the University (X), from about 2005 to about 2006, without authorization and against school policy. Applicant admits the allegation. He clarified in his Answer that he believes the downloading occurred on his personal computer. As mitigation he highlights that sufficient time has passed; that he had very little income while a student and could not afford to purchase the movies; and notes the last time he illegally

downloaded something was in October 2022. (Answer at 2.) He was reprimanded by the University (X) for copyright violations in December 2005. The reprimand advised him a second violation would result in serious consequences, which “at a minimum” included being charged with violation of computer policy, theft of intellectual property, and failure to comply with an official request. (Item 4 at 7, 16.)

SOR ¶ 2.b: Applicant illegally downloaded television shows, movies, e-books, and video games estimated to be valued at \$54,000, from his personal computer from about 2011 to present without authorization. Applicant admits the allegation. In his Response he clarifies that he has not been continuously downloading illegal content since 2011. He breaks down the times he illegally downloaded material and explains where there were multi-year gaps. He started downloading sometime between 2011 and 2015 and was “halted again” after his security clearance interview in July 2022 so it was “only 15 years total, with a 6-year break in the middle” vice 20 years. (Response at 2; Item 4.) He provides a detailed breakdown of the items in his Response to get to the \$54,000 figure and then notes that with subscription services the present-day value according to his breakdown is \$6,360. He notes he voluntarily reported these in his interview. (Response at 2; Item 3 at 17; Item 4 at 7, 16.) He explains in his Response that his “illegal downloading in general has just been a hobby, not a habit, which makes it easy to halt.” Now that he is aware of the implications to his security clearance, he has made efforts to halt any illegal downloading and deleted any illegal content from his computers. (Response at 3.)

SOR ¶ 2.c: Applicant loaded a Tor Internet browser onto his personal laptop, between 2015 and 2018 and accessed an illegal marketplace on the dark web where he viewed pictures on sale of women that were taken without their consent. Applicant admits the allegation. He states in his Answer and Response this was a onetime event that occurred one evening somewhere between 2015 and 2018. He thought “the dark web would have strange-but-benign websites to explore, though the links were sometimes unlabeled. That website was an “uncomfortable experience,” and he states he does not intend to go back to the Tor browser, the dark web, or to similar websites ever again. (Answer; Item 4 at 16-17.) There is no evidence that Applicant’s accessing the dark web was illegal. He stated in response to Government interrogatories that his accessing of the dark web was not part of a search for illegal content or to commit illegal acts. There is no evidence he used the dark web to sell or purchase illegal firearms, drugs, pornography, stolen passwords, hacked credit card account numbers, or other illegal items associated with the dark web. He stated in the Government interrogatories he thought the worst thing he saw on the dark web was a site selling pictures of adult women without their consent and affirmed he “did not purchase anything, nor view illegal content.” (Item 3 at 19.) He repeatedly denied to the investigator viewing any type of illegal pornography. (Item 4 at 17.)

SOR ¶ 2.d: Applicant illegally or when otherwise not authorized duplicated video games for LAN parties in about September 2001. Applicant admits the allegation. He states the video game duplication was a way to let everyone at the LAN party join in the gaming, so no one was left out. (Item 3 at 17.) He notes his video-game

duplication activities ended a long time ago and will not reoccur because, with streaming services, it is now easier to legally acquire games. He states he has “deleted any remaining illegal content on my technology, and [he] will not illegally download or duplicate anything in the future.” (Answer at 2.)

Guideline J

SOR ¶ 3.a: Information as set forth in subparagraphs 2.a through 2.d, above. Applicant admits the allegation. See the facts discussed in subparagraphs 2.a through 2.d above. As mitigation he cites the unusual circumstances of the downloading generally occurring when he was a student when he had little income. As an indication of his rehabilitation, he notes “stopped any kind of illegal or gray-area downloading [in October 2022], and [he] has no interest in continuing.” (Response at 3.)

As further mitigation Applicant offers in his Response that he is an honest person. He achieved “life rank” in the Boy Scouts. He abided by the alcohol laws and did not drink until he was 21 years old. He has never gotten a parking ticket or tried illegal drugs or marijuana. As a teaching assistant, he was entrusted with students’ grades. (Response at 3.)

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.

Eligibility for a security clearance 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 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.” 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. 15- 01253 at 3 (App. Bd. Apr. 20, 2016).

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.

Analysis

Guideline F: Financial Considerations

The security concern under this guideline is set out in AG ¶ 18:

Failure to live within one's means, satisfy debts, and meet financial obligations may indicate poor self-control, lack of judgment, or unwillingness to abide by rules and regulations, all of which can raise questions about an individual's reliability, trustworthiness, and ability to protect classified or sensitive information. . . . An individual who is financially overextended is at greater risk of having to engage in illegal or otherwise questionable acts to generate funds. . . . Affluence that cannot be explained by known sources of income is also a security concern insofar as it may result from criminal activity, including espionage.

This concern is broader than the possibility that a person might knowingly compromise classified information to raise money. It encompasses concerns about a person’s self-control, judgment, and other qualities essential to protecting classified

information. A person who is financially irresponsible may also be irresponsible, unconcerned, or negligent in handling and safeguarding classified information. See ISCR Case No. 11-05365 at 3 (App. Bd. May 1, 2012).

Applicant's admissions and the documentary evidence in the record establish the following disqualifying condition under AG ¶ 19:

(f) failure to file or fraudulently filing annual Federal, state, or local income tax returns or failure to pay annual Federal, state, or local income tax as required.

The following mitigating conditions under AG ¶ 20 are potentially applicable:

(a) the behavior happened so long ago, was so infrequent, or occurred under such circumstances that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or good judgment;

(b) the conditions that resulted in the financial problem were largely beyond the person's control (e.g., loss of employment, a business downturn, unexpected medical emergency, a death, divorce or separation, clear victimization by predatory lending practices, or identity theft), and the individual acted responsibly under the circumstances; and

(g) the individual has made arrangements with the appropriate tax authority to file or pay the amount owed and is in compliance with those arrangements.

AG ¶ 20(a) is not established. Applicant's unfiled tax returns are recent and did not occur under circumstances making them unlikely to recur. He has not demonstrated he has acted responsibly.

AG ¶ 20(b) is not established. Applicant attributed his tax issues to a misunderstanding of the tax laws. A condition possibly beyond his control but he did not file his Federal tax returns once he became aware he was wrong. He has not acted responsibly.

AG ¶ 20(g) is not established. Applicant offered no evidence he had filed his tax returns for the years in question or was working with a tax preparer as he claimed. His Federal tax-account transcripts reflect no tax returns filed. Applicant's repeated failure to fulfill his legal obligations does not demonstrate the high degree of good judgment and reliability required of those granted access to classified information. See, e.g., ISCR Case No. 15-08782 at 3 (App. Bd. Apr. 5, 2017).

Guideline M: Use of Information Technology

The security concern relating to the guideline for Use of Information Technology is

set out in AG ¶ 39:

Failure to comply with rules, procedures, guidelines, or regulations pertaining to information technology systems may raise security concerns about an individual's reliability and trustworthiness, calling into question the willingness or ability to properly protect sensitive systems, networks, and information. Information Technology includes any computer-based, mobile, or wireless device used to create, store, access, process, manipulate, protect, or move information. This includes any component, whether integrated into a larger system or not, such as hardware, software, or firmware, used to enable or facilitate these operations.

The guideline notes several conditions that could raise security concerns under AG ¶ 40. Three are potentially applicable in this case:

- (a) unauthorized entry into any information technology system;
- (d) downloading, storing, or transmitting classified, sensitive, proprietary, or other protected information on or to any unauthorized 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.

Over a period of many years, Applicant admitted he illegally downloaded proprietary information. He admits accessed an illegal marketplace on the dark web.

AG ¶ 41 provides conditions that could mitigate security concerns. I considered all of the mitigating conditions under AG ¶ 41 including:

- (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.

AG ¶ 40(a) is not established for the proprietary material (SOR ¶¶ 2.a-2.b). Applicant has not demonstrated he has acted responsibly. This illegal conduct is reoccurring. He was warned in 2005 by University (X) that his behavior not only violated its policy but was theft of intellectual policy. He continued the conduct up until as recently as 2022.

AG ¶ 40(a) is established SOR ¶¶ 2.c and 2.d. SOR ¶ 2.c was a one-time event, which occurred at least six years or more years ago. Sufficient time has elapsed since Applicant's behavior happened. His description of the event makes it unlikely to recur and does not cast doubt on his reliability, trustworthiness, or good judgment. SOR ¶ 2.d was

a pre-University (X) warning event and the conduct was distinct from the conduct alleged in SOR ¶¶ 2.a and 2.b. Sufficient time has elapsed since Applicant's behavior happened.

Guideline J, Criminal Conduct

AG ¶ 30 expresses the security concern for criminal conduct:

Criminal activity creates doubt about a person's judgment, reliability, and trustworthiness. By its very nature, it calls into question a person's ability or willingness to comply with laws, rules, and regulations.

31: The following disqualifying condition is potentially applicable as detailed in AG ¶

(b) evidence (including, but not limited to, a credible allegation, an admission, and matters of official record) of criminal conduct, regardless of whether the individual was formally charged, prosecuted, or convicted.

Applicant acknowledges his actions. The above disqualifying condition applies.

32: The following mitigating conditions are potentially applicable as detailed in AG ¶

(a) so much time has elapsed since the criminal behavior happened, or it happened under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment;

(c) no reliable evidence to support that the individual committed the offense; and

(d) there is evidence of successful rehabilitation; including, but not limited to, the passage of time without recurrence of criminal activity, restitution, compliance with the terms of parole or probation, job training or higher education, good employment record, or constructive community involvement.

AG ¶ 32(a), (c), and (d) do not apply. Applicant's criminal conduct continued despite a reprimand and continued until at least his security clearance interview in 2022. He has detailed his actions and the value of his criminal conduct. His criminal conduct continues to cast doubt on his current reliability, trustworthiness, good judgment, and willingness to comply with laws, rules, and regulations. The above mitigating conditions, individually or collectively, are insufficient to alleviate those concerns, given his history of using information systems to obtain proprietary or other protected information in violation of copyrights. He needs to establish a longer record of responsible behavior and

compliance with rules, regulations, and the law before his criminal conduct can be considered mitigated.

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 F, M, and J in my whole-person analysis and applied the adjudicative factors in AG ¶ 2(d). I have considered the accomplishments and traits Applicant cited in his Response. Because Applicant requested a determination on the record without a hearing, I had no opportunity to evaluate his credibility and sincerity based on demeanor. See ISCR Case No. 01-12350 at 3-4 (App. Bd. Jul. 23, 2003). After weighing the disqualifying and mitigating conditions under Guidelines F, M, and J and evaluating all the evidence in the context of the whole person, I conclude Applicant has not mitigated the security concerns raised by his conduct.

Formal Findings

I make the following formal findings on the allegations in the SOR:

Paragraph 1, Guideline F:	AGAINST APPLICANT
Subparagraph 1.a:	Against Applicant
Paragraph 2: Guideline M:	AGAINST APPLICANT
Subparagraphs 2.a and 2.b:	Against Applicant
Subparagraphs 2.c and 2.d:	For Applicant
Paragraph 3: Guideline J:	AGAINST APPLICANT

Subparagraph 3.a:

Against Applicant

Conclusion

I conclude that it is not clearly consistent with the national security interests of the United States to grant Applicant eligibility for access to classified information. Clearance is denied.

Charles C. Hale
Administrative Judge