DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 22-01946
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Adrienne Driskill, Esq., Department Counsel
For Applicant: *Pro se*

07/08/2024

_____

Decision

_____

TUIDER, Robert, Administrative Judge:

Applicant failed to mitigate security concerns regarding Guideline E (personal conduct), Guideline D (sexual behavior), Guideline F (financial considerations), and Guideline M (use of information technology). Eligibility for access to classified information is denied.

Statement of the Case

On September 3, 2021, Applicant completed and signed an Electronic Questionnaires for National Security Positions (SF-86) or security clearance application (SCA). On December 19, 2022, the Defense Counterintelligence and Security Agency Consolidated Adjudication Services (DCSA CAS) issued a Statement of Reasons (SOR) to Applicant under Executive Order (Exec. Or.) 10865, *Safeguarding Classified Information within Industry*, February 20, 1960; Department of Defense (DOD) Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (Directive), January 2, 1992; and Security Executive Agent Directive 4, establishing in Appendix A the *National Security Adjudicative Guidelines for Determining Eligibility for Access to Classified Information or Eligibility to Hold a Sensitive Position* (AGs), effective June 8, 2017.

The SOR detailed reasons why the DCSA CAS did not find, under the Directive, that it is clearly consistent with the interests of national security to grant or continue a

security clearance for Applicant and recommended referral to an administrative judge to determine whether a clearance should be granted, continued, denied, or revoked. Specifically, the SOR set forth security concerns arising under Guidelines E, D, F, and M.

On January 19, 2023, Applicant provided a response to the SOR, and he requested a hearing. On March 8, 2023, Department Counsel (DC) was ready to proceed. On March 15, 2023, DOHA assigned the case to me. On March 21, 2023, the Defense Office of Hearings and Appeals (DOHA) issued a notice of hearing, setting the hearing for April 18, 2023. The hearing was held as scheduled.

Department Counsel offered Government Exhibits (GE) 1 through 3, which I admitted without objection. Applicant testified and offered Applicant Exhibits (AE) A and B, which I admitted without objection. I held the record open until May 5, 2023, to afford Applicant an opportunity to submit additional evidence. (Tr. 55-59, 68-69) Applicant timely submitted AE C through S, which I admitted without objection. On April 27, 2023, DOHA received the hearing transcript (Tr.).

Some details were excluded to protect Applicant's right to privacy. Specific information is available in the cited exhibits and transcript.

Findings of Fact

Background Information

Applicant is a 66-year-old defense contractor, who has been employed in that capacity since August 2021. He seeks to retain his security clearance eligibility, which is a requirement of his continued employment. (Tr. 12-15, 20; GE 1)

Applicant was awarded a Bachelor of Science degree in history in May 1980. He was later awarded a Master of Business Administration degree in July 1994. (Tr. 15-16; GE 1) Applicant was previously married two times. His first marriage was from July 1980 to May 1984, and his second marriage was from June 1986 to July 1988. Both of those marriages ended by divorce. He married his third wife in March 1991, and has two adult children from his current marriage. (Tr. 16-18)

Applicant served on active duty in the U.S. Navy from 1980 to 1991. He affiliated with the Navy Reserve in 1991 and retired from the Navy Reserve in 2010, as a captain (pay grade O-6), having honorably served for 30 years. (Tr. 18-20; AE P)

Personal Conduct/Sexual Behavior/Financial Considerations/Use of Information Technology

The conduct that gave rise to these concerns occurred during Applicant's previous employment with a different defense contractor. He was employed by this defense contractor from July 2011 to May 2021. (Tr. 43; GE 1) In May 2021, Applicant was

involuntarily terminated by this employer. (Tr. 48-51) The SOR alleged four concerns that arose from this termination:

SOR ¶ 1.a (Personal Conduct) – terminated for misconduct in violation of company policies: (1) timesheet accounting, (2) employee misconduct and disciplinary action, (3) information technology acceptable use policy, and (4) company standards of ethics and business conduct;

SOR ¶ 2.a (Sexual Behavior) - between March 2021 and April 2021, Applicant used his company computer to view pornographic images on a recurring basis;

SOR ¶ 3.a (Financial Considerations) – between March 2021 and April 2021, Applicant mischarged approximately 15.5 hours of time to a direct program that were not worked based on recurring inappropriate use of his company computer during working hours; and

SOR ¶ 4.a (Use of Information Technology) - the SOR cross-alleged SOR ¶¶ 1.a and 2.a under Use of Information Technology.

In Applicant's SOR response, he admitted SOR ¶¶ 1.a and 4.a, and denied 2.a and 3.a. In his SOR response, he also provided mitigating information. His admissions are accepted as findings of fact.

During the March 2021 to April 2021 timeframe, which was during the COVID-19 lockdown, Applicant was assigned to an 8,000 square foot workspace with "two other people routinely in the building . . [so] social distancing . . . was never an issue." (Tr. 21-22, 46-48) He described his work responsibilities to include, but not limited to, managing two large separate Government contracts that required Teams meetings, as well as access to navy.mil course development programs. He found these requirements challenging due to firewall access issues, discussed below. (SOR Answer)

Without access or limited internet access, Applicant was having trouble getting his work done and became increasingly frustrated. He stated that he did not have any local support as most other company employees were working on another coast and he was not getting the assistance he needed. (GE 2, May 24, 2022 Office of Personnel Management Personal Subject Interview (OPM PSI), p. 2) In April 2021, Applicant's company information technology (IT) department discovered that he had been accessing pornographic sites on his company-issued computer. (Tr. 22-24) Applicant stated:

> . . . my issue with IT was I could never get on the .mil sites that I needed to do our work and they did not respond to calls to fix and I just thought, well, maybe, you know – not a good decision on my part, but – I said, well maybe if I do something like this, they will notice that and call me and say, "Can I help you," and they didn't. . . . So pornographic sites, even any firewall will block those, but search engine stuff is what they found and – . . . I got one phone call from two people I've never met, heard of, and it was a search engine discussion. . . . They could see what you searched - - (Tr. 23-24)

Applicant stated that he lost his local IT support when company employees began teleworking as a result of the COVID-19 epidemic.

Applicant's employer conducted an internal audit time-charging review, and by memorandum dated May 6, 2021, reported in part the following:

> Based on the interviews conducted and review of available documentation (network activity logs, computer log-on/off activity logs), we have concluded that [Applicant] misused [company] IT equipment on a recurring basis by searching and viewing pornographic images on a recurring basis from March 1, 2021 to April 21, 2021, which is a violation of [company] policy IT 100 (Information Technology Acceptable Use Policy).
>
> In addition, based on the recurring nature of the misuse, up to 2.5 hours per day from March 1, 2021 to April 21, 2021, IA noted that [Applicant] appears to have mischarged time to a direct program, which is in violation of FA 701 (Timesheet Accounting). Specifically, it appears that [Applicant] recorded 15.5 hours from March 1, 2021 to April 21, 2021 that were not worked based on a recurring inappropriate use of his [company] computer during working hours. (GE 3, p. 4)

Applicant stated that he wanted the IT department to see that he was able to access pornographic sites and that he was unable to access his .mil accounts or accounts that he needed to do his job "because the firewall keeps blocking me, which made it really challenging to do the research kind of work that I need to do for the documents I prepare. So it was a misguided effort to get somebody to fix it. They were 3,000 miles away, probably in their parents' basement." (Tr. 24) As an example, he would use a search term "nude" and added , "If you clicked on the results, then it brought up a firewall." So it was just – again, I was trying to just get somebody to talk to me about it. Which they did, but after the fact." (Tr. 26)

Department Counsel (DC) queried the Applicant further about the viewing of pornographic images. She attempted to clarify whether Applicant was able to make it past the firewall or whether the firewall did not exist for certain sites. Applicant stated, "If you do a search, an image search, it will bring up the image. . . . And then – but if you click on whatever the image is, then it takes you to the site which is what – which I really didn't have time to do." (Tr. 26-27) Applicant stated that he did not view videos, "because, again, videos don't run off the – at least my – my basic understanding of IT is that videos don't run off of the browser search. It will take you to I think whatever the site you're searching." (Tr. 27)

> DC: Well, in for example Government Exhibit 3, page 4, they (Applicant's employer) note that it would be up to 2.5 hours per day that they're saying you were searching or viewing pornographic images. So that – the way I'm reading that means either you're spending up to that amount of time searching or you had either images or videos pulled up during the duration

of that time, this 2.5 hours we're talking about. Can you kind of explain that to us?

Applicant: I'd bring it up and leave it so they – you know, so it was open.

DC: And when you say it was open, what are you – tell us what you're referring to. What was open?

Applicant: The browser search engine was open type stuff.

DC: Okay.

Applicant: Again, open in the background or minimized.

DC: And explain to me how – how you envisioned having that browser result sitting there, how is that going to raise issues with a firewall?

Applicant: Well, I mean, ultimately it worked because they eventually called me. It just wasn't real time. It wasn't – it wasn't – it was – the whole issue of getting onto the required .mil account sites was a – was a hit-or-miss. Five days, it would work one day. Tr. 28-29)

Applicant stated what he was "trying to prove" was that the firewall would not let him get him get to a navy.mil account, i.e. the firewall would block that account, but would not block things such as pornographic web sites. (Tr. 30) Applicant stated that he "called IT" or "left a ticket number" or "sent it (service request) by email" to resolve the firewall issue and "[a]nd never got any resolution on it." Applicant stated he contacted his IT department "probably weekly" to resolve the firewall problem. (Tr. 31, 46) Applicant did not raise these issues with his supervisor stating, "cause I kept – I kept getting enough done that I didn't miss any deadlines for it." (Tr. 31, 46) He did not provide a copy of the ticket or emails to IT for inclusion in the hearing record.

Applicant acknowledged that between March 2021 and April 2021, he was aware that it was against company policy to use his work computer to view pornography. (Tr. 32)

DC: Okay, And even assuming that, you know, everything you're saying is true and you were trying to raise concerns with IT, can you see the concern about your judgment and violation of policy with the way that you approached trying to –

Applicant: I did. I admit that up front. It was a dumb thing to do – driven obviously by frustration on my part and probably a little bit by the pandemic, lack of working – frustration. Yeah, I – it was stupid. (Tr. 32-33)

DC: And they (employer) also accused you of – in the – or [employer] accused you mischarging time for the amount of hours that they believed you to be searching or viewing pornography. And you deny that; right?

Applicant: I do.

DC: Why do you deny that?

Applicant: Well, like I said, I was working on – so – I'm trying to remember. That's over two years ago. Again, I was – I was working actively on at least four of the [project description] at the same time. I was helping out on a couple other environmental assessments, environmental impact statements. And I also – because I also picked up management of programs from my coworker who went back on active duty. I was managing a contract in [state] with the [Navy command] and something else – and closing out another contract that we had locally. All of that was without any billable hours for me. So – not doing pro bono, but I was doing a lot of program management work without being compensated. So I had more work to do than I had time to do. (Tr. 33-34)

Applicant's employer never tried to recoup back pay for the 15.5 hours Applicant reportedly did not work based on recurring inappropriate use of his computer during working hours. Applicant stated, "Because I met all the deliverables that was required for all of them. Applicant stated that he was never given the opportunity to prove that he was working during those hours. (Tr. 34) Applicant stated he was able to complete his work while his browser with pornographic websites was usually minimized. (Tr. 51-52)

Referring to Government Exhibit 2, page 11, which was Applicant's May 24, 2022 OPM PSI, DC queried him further.

DC: Because in your interview, you described trying to access random websites to prove the absurdity of what was being blocked. And the largest paragraph on that page, sort of in the center, it said – and this is her words (investigator), not yours, but it said – it says, "The subject started accessing random sites on the Internet that should be blocked, trying to show the absurdity of what was being blocked, which is what he accessed to that issue. Subject would put up websites with access on one of his computer screens while he was doing his actual work on the other screen. Subject was not accessing any particular websites and was just opening websites that he felt should have been blocked by the firewalls and weren't. Subject would open the websites and then ignore them while he worked, because he could."

And that makes it sound more like you were clicking on actual websites. Is – were you – did you ever have actual websites pulled up or just search engine results?

Applicant: I don't recall.

DC: Okay. Were there other, apart from – I'm sorry. Did you –

Applicant: I'm just – it was – I don't remember, to be honest with you. (Tr. 34-35)

Applicant stated he would need an example of a non-pornographic website he may have tried to search in order to say, "yes or no," that he tried to access to prove the absurdity of the firewall. He stated, "I was just trying to use what I knew I shouldn't – I shouldn't be able to get to and I did." (Tr. 36) Applicant could not "say specifically" whether at the time he conducted these searches two other co-workers were in the office spaces. (Tr. 37) Applicant did not tell anyone else "at work during that time" that he was attempting to get IT's attention to the firewall problem he was experiencing. (Tr. 37)

DC: Okay. Why did you do it (access pornographic websites) repeatedly over the course of just under two months?

Applicant: I'm trying to – I don't remember what I was working on then, but it was probably – again, I'm just kind of guessing – it was probably a culmination of a project that I needed to finish that I couldn't get access to things I needed.

DC: Uh-huh.

Applicant: But I – I couldn't tell you for sure. (Tr. 37-38)

Applicant stated that he lost his local IT support in 2020 when company employees vacated their workspaces and began teleworking as a result of the COVID-19 epidemic. (Tr. 43-45)

Applicant commented:

The phrase, you know, one "Aw shucks" wipes out a whole bunch of "Attaboys," but it did 'cause I was very successful with [previous employer], although I was – like I told the investigator that was for my clearance, it was getting frustrating in that job anyway, not – not for the IT issues, but for some of the other changes in how things were going. I probably would have left anyway. If I would have found this job earlier, I would have went earlier. (Tr. 52-53)

Character Evidence

Applicant discussed his job description in considerable detail. To describe his duties and responsibilities would reveal identifying information. Suffice it to say, he is providing a very valuable and essential service to his defense contractor employer. *See* pages 38-43, 53-55. He provided a current job description that further elaborated on his

job duties. (AE B) Applicant's 2022 performance evaluation gave him the highest rating, "Excelling." (AE A)

Post-hearing, Applicant submitted numerous emails and documents that discussed his professional and civic involvement. He also provided documentation showing that he had completed various security training courses**. (**AE C – AE S)

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 conjunction with the factors listed in AG ¶ 2 describing 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 clearance 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

Personal Conduct

AG ¶ 15 articulates the security concern for personal conduct:

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

AG ¶ 16 describes two conditions that could raise security concerns and may be disqualifying in this case:

> (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 that individual may not properly safeguard classified or sensitive information; and
>
> (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: . . . (4) evidence of significant misuse of Government or other employer's time or resources.

The record raises the disqualifying conditions in AG ¶¶ 16(c) and 16(d)(4). AG ¶ 16(c) is not established because there is credible adverse information in several adjudicative issue areas that is sufficient for an adverse determination under other guidelines. AG ¶ 16(d)(4) applies requiring additional inquiry about the possible applicability of mitigating conditions.

In ISCR Case No. 10-04641 at 4 (App. Bd. Sept. 24, 2013), the DOHA Appeal Board explained Applicant's responsibility for proving the applicability of mitigating conditions as follows:

> Once a concern arises regarding an applicant's security clearance eligibility, there is a strong presumption against the grant or maintenance of a security clearance. *See Dorfmont v. Brown*, 913 F. 2d 1399, 1401 (9th Cir. 1990), *cert. denied*, 499 U.S. 905 (1991). After the Government presents evidence raising security concerns, the burden shifts to the applicant to rebut or mitigate those concerns. *See* Directive ¶ E3.1.15. The standard applicable in security clearance decisions is that articulated in *Egan*, *supra*. "Any doubt concerning personnel being considered for access to classified information will be resolved in favor of the national security." Directive, Enclosure 2 ¶ 2(b).

AG ¶ 17 includes three conditions that could mitigate the security concerns arising from Applicant's personal conduct:

> (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 obtaining 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.

AG ¶¶ 17(c), 17(d), and (e) are partially applicable. However, Applicant did not sufficiently establish these mitigating conditions given the serious lapses of judgment he exercised over a two-month period between March 2021 and April 2021, when he used his company computer to view pornographic images on a recurring basis. Furthermore, his excuse for this misconduct is that he intended to flag the lack of IT support and the improper blocking of Navy websites he needed for his work. This explanation is not credible. His failure to take responsibility for his poor decisions shows a lack of rehabilitation. While Applicant acknowledged his lapses in judgment, apart from his assurances of remorse and completion of security training, there is no record evidence to suggest such behavior will not recur.

Sexual Behavior

AG ¶ 12 articulates the security concern for sexual behavior:

> Sexual behavior that involves a criminal offense; reflects a lack of judgment or discretion; or may subject the individual to undue influence of coercion, exploitation, or duress. These issues, together or individually, may raise questions about an individual's judgment, reliability, trustworthiness, and ability to protect classified or sensitive information. Sexual behavior includes conduct occurring in person or via audio, visual, electronic, or written transmission. No adverse inference concerning the standards in this Guideline may be raised solely on the basis of the sexual orientation of the individual.

AG ¶ 13 describes two conditions that could raise security concerns and may be disqualifying in this case:

> (c) pattern of compulsive, self-destructive, or high-risk sexual behavior that the individual is unable to stop; and
>
> (d) sexual behavior that causes an individual to be vulnerable to coercion, exploitation, or duress.

The record establishes the disqualifying conditions in AG ¶¶ 13(c) and (d), requiring additional inquiry about the possible applicability of mitigating conditions.

AG ¶ 14 includes four conditions that could mitigate the security concerns arising from Applicant's sexual behavior:

> (b) the sexual behavior happened so long ago, so infrequently, or under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or judgment;
>
> (c) the behavior no longer serves as a basis for coercion, exploitation, or duress;
>
> (d) the sexual behavior is strictly private, consensual, and discreet; and
>
> (e) the individual has successfully completed an appropriate program of treatment, or is currently enrolled in one, has demonstrated ongoing and consistent compliance with the treatment plan, and/or has received a favorable prognosis from a qualified mental health professional indicating the behavior is readily controllable with treatment.

AG ¶ 14(c) applies. Applicant used his company computer to view pornographic images on a recurring basis between March 2021 and April 2021 in his workspace. In doing so, he exercised very poor judgment. His behavior no longer serves as a basis for coercion because cognizant supervisors know about it. He completed security training, and he is well aware of the consequences of viewing pornography on a government computer. I do not believe he would engage in such behavior in the future. Given his

demonstrated lack of remorse, however, the lack of discretion and poor judgment he exhibited remain unmitigated concerns.

Financial Considerations

AG ¶ 18 articulates the security concern for financial problems:

> 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. Financial distress can also be caused or exacerbated by, and thus can be a possible indicator of, other issues of personnel security concern such as excessive gambling, mental health conditions, substance misuse, or alcohol abuse or dependence. An individual who is financially overextended is at greater risk of having to engage in illegal or otherwise questionable acts to generate funds.

AG ¶ 19 describes one condition that could raise security concerns and may be disqualifying in this case:

> (d) deceptive or illegal financial practices such as embezzlement, employee theft, check fraud, expense account fraud, mortgage fraud, filing deceptive loan statements and other intentional financial breaches of trust.

The record evidence establishes disqualifying condition AG ¶ 19(d) requiring additional inquiry about the possible applicability of mitigating conditions.

AG ¶ 20 includes three conditions that could mitigate the security concerns arising from Applicant's financial misconduct:

> (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;
>
> (c) the individual has received or is receiving financial counseling for the problem from a legitimate and credible source, such as a non-profit credit counseling service, and there are clear indications that the problem is being resolved or is under control.

None of these mitigating conditions fully apply. The Government's evidence documents that Applicant mischarged approximately 15.5 hours of time to a direct program that were not actually worked, during his recurring use of his company computer to access pornographic websites during working hours. Although Applicant claims that he completed his work assignments, he placed himself in an unjustifiable position of having open pornographic sites, albeit allegedly "minimized", at the same time he billed hours to a client. His explanation that he did not view these sites for 15.5 hours is not credible. There is no evidence to support his claim that he did not view pornography on his company computer during those duty hours. His employer's IT department found that up to 2.5 hours might have been mischarged because of Applicant's searching and viewing pornographic images. I have given deference to Applicant's previous employer's internal investigation and characterization of events in these proceedings. While it is unclear how much timecard fraud occurred, I am confident that some occurred in this case.

Use Of Information Technology

AG ¶ 39 articulates the security concern for 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.

AG ¶ 40 described one condition that could raise security concerns and may be disqualifying in this case:

(e) unauthorized use of any information technology system.

The record establishes the disqualifying condition in AG ¶ 40(e), requiring additional inquiry about the possible applicability of mitigating conditions.

AG ¶ 41 includes four conditions that could mitigate the security concerns arising from applicant use of information technology:

> (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;
>
> (b) the misuse was minor and done solely in the interest of organizational efficiency and effectiveness;

(c) the conduct was unintentional or inadvertent and was followed by a prompt, good-faith effort to correct the situation and by notification to appropriate personnel; and

(d) the misuse was due to improper or inadequate training or unclear instructions.

None of the mitigating conditions are fully applicable. Applicant was experienced and well versed in matters of security. The record evidence documents his repeated accessing and searching of pornographic sites. Company records use the term "searching and viewing pornographic images." This is very different from someone who does this once, realizes the error of their ways, and never does it again. Applicant continued to engage in this inappropriate behavior until he was caught. This recurring and repeated searching and accessing of pornographic sites, in and of itself, raises serious concerns, particularly as it pertains to judgment.

Whole-Person Concept

Under the whole-person concept, the administrative judge must evaluate an applicant's eligibility for a security clearance by considering the totality of the applicant's conduct and all the 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), "[t]he ultimate determination" of whether to grant a security clearance "must be an overall commonsense judgment based upon careful consideration of the guidelines" and the whole-person concept. My comments under Guidelines E, D, F, and M are incorporated in my whole-person analysis. Some of the factors in AG ¶ 2(d) were addressed under those guidelines but some warrant additional comment.

When evaluating this case, two things come to mind. Either Applicant is telling the truth and exercised a severe lack of judgment over an extended period of time by accessing pornographic sites during a two-month period to get the attention of and demonstrate to his company's IT department that his company had a problem with their firewalls. Alternatively, Applicant is lying about intentionally accessing pornographic sites during work hours on his company-issued computer and caused his company to bill clients for the time when he was accessing these sites. In either case, he did so in clear violation of company policy. Applicant failed to provide proof that he notified his supervisor or IT personnel that he was experiencing these firewall problems that he claims inhibited

his ability to complete his job assignments. The record evidence and objective assessment of his credibility establish that Appellant lied when he provided a false narrative about his reasons for going to pornographic sites during the duty day. HIs false statements and attempted justifications at his hearing show a lack a rehabilitation and weigh against continuing his national security eligibility for access to classified information.

With that said, Applicant's record of accomplishments is extraordinary. He has dedicated his entire adult working life to the national defense as a uniformed officer and later as a defense contractor. He is highly regarded by his superiors as a true professional and someone who can be relied upon. For privacy considerations, this part of Applicant's background is not discussed in further detail.

I have carefully applied the law, as set forth in *Department of the Navy v. Egan*, 484 U.S. 518 (1988), Exec. Or. 10865, the Directive, the AGs, and the Appeal Board's jurisprudence to the facts and circumstances in the context of the whole person.

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
Subparagraph 1.a:	Against Applicant
Paragraph 2, Guideline D:	AGAINST APPLICANT
Subparagraph 2.a:	Against Applicant
Paragraph 3, Guideline F:	AGAINST APPLICANT
Subparagraph 3.a:	Against Applicant
Paragraph 4, Guideline M:	AGAINST APPLICANT
Subparagraph 4.a:	Against Applicant

Conclusion

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

_____
ROBERT TUIDER
Administrative Judge