DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 20-00898
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Bryan Olmos, Esq., Department Counsel
For Applicant: Orest J. Jowyk, Esq.

03/25/2022

_____

Decision

_____

MURPHY, Braden M. Administrative Judge:

Applicant was terminated from his employment in May 2017 after a company investigation determined that he had accessed, downloaded, or stored pornography on company computer systems, in violation of company policy. Applicant acknowledged an interest in pornography, but denied accessing any pornography on company computers. He believes instead that such evidence was fabricated in an attempt to manufacture a reason for his termination. During that employment, Applicant also engaged in a romantic relationship with a subordinate employee for a period of time, which was found to be additional grounds for his termination. While Guideline D security concerns are mitigated, Applicant did not provide sufficient evidence to mitigate the security concerns under Guidelines M and E. Eligibility for a security clearance is denied.

Statement of the Case

Applicant submitted a security clearance application (SCA) on September 25, 2018. On March 15, 2021, the Department of Defense (DOD) issued Applicant a Statement of Reasons (SOR), alleging security concerns under Guideline D (sexual conduct), Guideline

M (use of information technology), and Guideline E (personal conduct). DOD issued the SOR 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 Security Executive Agent Directive 4 (SEAD 4) *National Security Adjudicative Guidelines for Determining Eligibility for Access to Classified Information or Eligibility to Hold a Sensitive Position* (AG), which became effective on June 8, 2017.

Through his original counsel, Applicant answered the SOR allegations on April 1, 2021, and requested a hearing before an administrative judge from the Defense Office of Hearings and Appeals (DOHA). The case was assigned to me on September 7, 2021. On December 10, 2021, DOHA issued a notice scheduling the hearing for January 20, 2022.

The hearing convened as scheduled. It was conducted via video-teleconference through an online platform. Department Counsel submitted Government's Exhibits (GE) 1 through 4, all of which were admitted without objection. Applicant testified and submitted an affidavit, which was marked as Applicant's Exhibit (AE) A and admitted without objection. Two other witnesses also testified for Applicant. DOHA received the hearing transcript (Tr.) on February 1, 2022.

Findings of Fact

As to SOR allegation ¶ 1.a, and the cross-allegations (SOR ¶¶ 2.a and 3.b), Applicant admitted that his employment was terminated as alleged, but he otherwise denied the allegations. He denied the allegation at SOR ¶ 3.b. His answers also included narrative explanations. Applicant's admissions and explanations are incorporated into the findings of fact. After a thorough and careful review of the pleadings and exhibits submitted, I make the following findings of fact.

Applicant is 65 years old. He and his second wife married in 1991. She moved across the country to take a new job in summer 2011; he filed for divorce in June 2012, and moved out of the marital home soon thereafter. (AE A at ¶ 16; Tr. 26, 76-77, 105-106) They divorced in September 2014. (GE 1 at 22-23; Tr. 75-76) Applicant remarried in June 2017. (GE 1 at 21)

Applicant has a master's degree and a Ph.D., both in nuclear engineering. (Tr. 24) He has been employed in the defense industry, with security clearances, for most of the last 35 years, since at least 1987. (GE 1 at 14-17, 53-54, Tr. 25) He said he did not hold a clearance at the time of the hearing. (Tr. 8)

From 2002 until May 2017 when he was terminated, Applicant worked for company 1. At the time, Applicant was the company's chief strategy and technology officer, as well as acting senior vice president and general manager. (GE 1; Tr. 98) Applicant has worked for his current employer since July 2018, and is now the chief operating officer. (GE 1 at 14; Tr. 102)

In September 2015, company 1 was acquired by a venture capital firm. A month later, half of Applicant's responsibilities were re-organized under someone else. He came to believe he was being undermined. In January 2016, Applicant refused to sign an annual ethics certification because he believed the business plan submitted to the venture capital firm was inaccurate. The company's general counsel, Mr. F., requested that Applicant file a confidential ethics complaint. The company's human resources (HR) director nonetheless soon learned about it. (AE A at ¶¶ 20-28; Tr. 29-31)

Applicant then offered his resignation but was soon promoted to chief strategy and technology officer, with primary responsibility for company 1's business with the U.S. Navy. AE A at ¶¶ 29-31; Tr. 72-73, 103) At the height of his responsibilities, Applicant had 900 full-time and part-time employees. (Tr. 74) In the process, another employee, Mr. C, was demoted, and Applicant became Mr. C's supervisor. (AE A at ¶ 34; Tr. 31-32) For the next several months, Applicant had a dispute with his superiors over the fairness of his performance bonus and salary increase, especially compared with Mr. C. He also sought to remove Mr. C due to ethics violations and sexual harassment complaints against Mr. C made by female employees. (AE A at ¶¶ 34-50; Tr. 32-36)

In May 2017, company 1 conducted an investigation into Applicant's workplace conduct, including a romantic relationship with a subordinate employee in Applicant's chain of command, and the company's discovery that Applicant had accessed and downloaded an extensive collection of pornography on company computer systems. (GE 4) This alleged conduct, as detailed in GE 4, is the basis for the allegations and cross-allegations in the SOR. The Government offered GE 4 with redactions, as they received it from company 1. (Tr. 18)

Government Exhibit 4 was prepared by company 1's general counsel, Mr. F. Review of the report indicates that the investigation was initiated when Mr. F learned of the relationship between Applicant and the subordinate employee in 2017, after the employee raised concerns about working for Applicant, given their prior romantic involvement. (GE 4 at 2)

The company's investigation concluded that Applicant had pursued and engaged in a long-term relationship with a subordinate employee through early 2016. The report noted that e-mails between Applicant and the employee also showed at various points that he expressed his love for her, pressed her to commit to him, and provided her gifts, such as flowers and jewelry. (GE 4 at 4) The company concluded that he did not report the relationship to the company, and did not take other steps to mitigate any risks to the company, such as potential claims of sexual harassment or a hostile workplace environment, or favoritism towards the subordinate employee in the promotion process, either real or perceived. (GE 4 at 1-2, 4)

Applicant acknowledged that between August and December 2012, he had a consensual sexual relationship with S, an administrative assistant at company 1. He said S reported to a manager who reported to Applicant. He said that S initiated the relationship.

He said the sexual relationship lasted between August and December 2012, and did not resume after that. (AE A at ¶ 2-3; Tr. 26, 48, 77-78, 81-82, 84, 104-105)

Applicant said that he was never S's direct supervisor, but he said he approved promotions or raises recommended to him by her direct supervisor. (AE A at ¶ 14; Tr. 27, 49, 79-81) Applicant said that S remained in his chain of command until he was promoted out of the organization. (Tr. 50) He is not aware of a company 1 policy prohibiting a romantic relationship such as between himself and S. (Tr. 89)

Applicant said he confirmed the relationship to company 1's human resources director in 2013 once he was asked about it. He said that that the CEO told him that he should not have mentioned the relationship to a former company 1 employee, but that the company took no disciplinary action against Applicant at the time. (AE A at ¶¶ 4-7; Tr. 27, 52-53, 81, 103-104)

To separate himself from S, Applicant moved to another branch office in the area for about nine months; he also moved to another area office on two occasions, also to avoid S. Applicant testified that their sexual relationship did not extend beyond late 2012, though he said that both parties later sought to renew the relationship, for different reasons, between 2013 and 2015. Applicant testified that he wanted a more public relationship, and while she at times sought to renew their affair, she wished to remain married. (AE A at ¶¶ 8-13; Tr. 28, 52-54, 81-86, 106-111)

Applicant and his third wife met online in about 2015, became serious by early 2016 and married in 2017. (Tr. 89-90) They now live in a state across the country from where Applicant lived when he was at company 1, and are happily married. Applicant regrets the relationship with S and says there is no chance it will recur. (Tr. 47)

The rest of GE 4 concerns company 1's discovery that Applicant had downloaded, accessed, or stored "an extensive collection of pornography" on company-owned computer systems. Mr. F reported that on Tuesday, May 2, 2017, he entered Applicant's office during normal business hours while Applicant was travelling and found an external hard drive (EHD) on Applicant's desk. The report indicates that Mr. F opened the drive and viewed, or attempted to view, its contents. (GE 4 at 2)

In GE 4, Mr. F reported that the contents of three directories on the drive included over 100 playlists and over 100 video clips, saved to the directory in 2009 or 2010, many with sexually suggestive file names, as well as several hundred files, in Microsoft Word or Acrobat PDF format, some of an "explicit sexual nature," saved to the directory between 2007 and 2012. (GE 4 at 2-3)

The report indicates that Mr. F found these materials on Tuesday, May 2, 2017. (GE 4 at 2) The report also indicates that "based on these preliminary findings, on Monday, May 1, 2017, [sic] [Mr. F] asked the IT department to remotely access Applicant's [company 1-provided] computer" for additional evidence of risk to the company. (GE 4 at 3) (In seeking to undermine GE 4. Applicant and his counsel drew attention to this date discrepancy,

noting that Mr. F could not have sought assistance from the IT department the day before he found the inappropriate materials on the EHD. This date discrepancy is unexplained)

On May 3, 2017, Company 1's IT department notified Mr. F that they had found 50 gigabytes of "suspect video and movie files" found to contain file names suggesting they contained pornographic images, videos, and documents. Later that day, they notified Mr. F that "the offending files had been deleted by someone." The IT department also found a spreadsheet titled "Recent Downloads list 4-8-17" and a document detailing Applicant's personal account information for his membership on an adult website, sent to his personal e-mail address. Mr. F printed the spreadsheet, which identified 280 unique files, identified by words and descriptors that "strongly suggest the existence of hardcore pornography." GE 4 at 3) According to GE 4, a review of Applicant's e-mail files also showed that from his company account to his personal email, he sent "a 50-page document titled 'movielist.txt' that identified the contents of an additional portable device containing more than 1,300 files," many with file names containing explicit pornographic terms. (GE 4 at 4) The memo from Mr. F is in the record (GE 4), but the underlying computer data is not.

Company 1's internet policy prohibited "browsing explicit pornographic . . . or other sites determined to be inappropriate" and "posting, sending, or acquiring sexually explicit or sexually oriented . . . or other material determined to be inappropriate." (GE 4 at 4) Applicant testified that he was "absolutely" aware of that policy, since he had reviewed it, commented on it, and approved it. (Tr. 97-98)

On May 8, 2017, Applicant attended a morning meeting in a conference room at company 1's offices. (Tr. 40) He also had an office there. He believes that, when he left his office for the meeting, his personal EHD was in his briefcase. (AE A at ¶¶ 60-62; Tr. 40-41) When Applicant arrived at the meeting, Mr. C was there, though he left the room for 10-15 minutes before coming back. (AE A at ¶ 62; Tr. 41)

Applicant was away from his office all day, until about 6 PM. When he returned, the company general counsel, Mr. F, and the chief operating officer, Mr. S., entered his office to talk to him. They told him that a large amount of pornography had been found on his company tablet. They did not show him evidence of what they had found. AE A at ¶ 65; Tr. 42-43)

Applicant noticed that both his personal EHD and the company EHD were on his desk. (Tr. 42) He said Mr. F picked up both the personal and company EHD, saw a label on the personal item and put it down. (Tr. 71, 94) Applicant's company tablet and company EHD were seized, but they did not access the personal EHD at that time. (Tr. 71) Applicant was told he was being placed on administrative leave. He packed his personal items and was escorted from the building. (AE A at ¶ 65; Tr. 43-44)

The May 13, 2017 company 1 report concluded that "as the senior-most manager leading a significant share of [company 1's] business, [Applicant's] behavior and judgment sets the wrong example and tone at the top, violates our Policies and Code, and exposes [company 1] to significant legal and reputational risk." (GE 4 at 4) Mr. F's conclusion,

following consultation with outside employment counsel, was that Applicant should be immediately terminated for cause. (GE 4 at 4)

Applicant was called to a meeting on May 15, 2017, with all of the company's executive managers. Mr. F told him that "they found a large amount of pornographic material on my [company 1] tablet" and that he was being dismissed as a result. (Tr. 44) Then and subsequently, Applicant requested to be shown what was found but was rebuffed. (Tr. 45) The record does not include a termination letter from company 1, but it is reasonable to infer that he was terminated for cause given the findings and conclusions in in GE 4 and the fact that he was terminated soon thereafter.

Applicant's termination led to an incident report in the Defense Department's JPAS. (GE 3). I therefore infer that he had a clearance at the time, as otherwise an incident report in JPAS would not have been made.

Applicant testified that company 1 had issued him a Microsoft "tablet" computer, as well as a company-issued external hard drive (EHD), to back up the tablet and to provide space for an e-mail archive. The tablet was not suitable for working at home, so he used his personal computer. He also used a personal EHD to transfer company 1 information (work files) between his personal home computer and his work tablet. (AE A at ¶¶ 51-55; Tr. 36-38, 55-58, 96, 107-108)

Applicant's personal EHD and the company-issued EHD looked alike, so he labeled the personal EHD as such. (AE A at ¶ 56, Tr. 58) He would connect the personal EHD to the company tablet only when transferring company data to work on at home, or when transferring company data back to his company tablet after he did so. Otherwise, he kept his personal EHD in his briefcase. (AE A at ¶¶ 57-58; Tr. 38-39, 64) He said he was careful to delete proprietary information from both his personal EHD and his personal home computer. (Tr. 59)

Applicant testified that he was asked to keep the company EHD at his office and not "carry it around" because it contained company proprietary information. (Tr. 37) He acknowledged transporting the company EHD between his various company workspaces (he had three offices) but did not take it home or on travel. (Tr. 55-56, 59, 107-108) He was not comfortable using a "thumb drive" for fear of losing it. (Tr. 60-61)

Applicant acknowledged viewing pornography on his personal computer beginning after he and his second wife separated in 2011. He said he did so only at home. (Tr. 95, 107) He testified that he did not use his personal EHD for that purpose. (Tr. 91-92). However, in AE A, his affidavit, Applicant stated that, "on my personal EHD, I stored images that could be described as pornographic" but not illegal. (AE A at ¶ 55)

Applicant acknowledged that it was "possible" that he had transferred or downloaded pornographic files from his personal computer to his personal EHD. He testified, "I don't specifically recall purposely doing it, but I ran backups. It was possible that the scope of the backup included some of those files. . . . I can't say for certain that I did

not." (Tr. 61-62) "Yes, it's possible. I certainly didn't do it intentionally." (Tr. 96-97) He maintained a "robust firewall" for virus and malware protection on his personal computer and believed it to be better than what the company used. (Tr. 62) Applicant acknowledged that he could have accessed his personal files from the company tablet. (Tr. 65)

Applicant denied storing pornography on company assets: "All I can say is I did not put it there." (Tr. 95-96) He denied downloading and saving pornographic content on company assets during working hours. (Tr. 65) Applicant "absolutely" denied using a company 1 computer, tablet, or EHD to view pornography. (Tr. 92) "I did not put pornography on [company 1's] owned tablet," or on any piece of company computing equipment. (Tr. 38, 47-48, 66) Applicant "never stored or accessed any inappropriate personal images, videos, or documents" on the company 1 tablet, the company EHD, or through any company technology. (AE A at ¶ 59; Tr. 54-55)

Applicant did not recall e-mailing a 50-page movie list file from his work e-mail to his personal e-mail (as noted in GE 4) and said, "I don't know why I'd do it. . . . It just doesn't make sense to me." (Tr. 98-99) He testified that he would have no reason to put files such as "recent downloads list 4/8/17" or "movielist.txt" on the company 1 tablet. (Tr. 67) He acknowledged, however that it was "possible" that he had a movie list file or a recent download file concerning pornographic video or imagery on his personal computer, and that he "may have" maintained such a list on his personal computer, but did not recall specifically. "Because certainly in 2017 I was living with my current wife. So there may well have been files created at an earlier date. Say before June of 2016." (Tr. 67-68) He said he did not remember creating such a document, and did not know why it would be on his work computer. (Tr. 99, 100) He acknowledged, however, that "I might have created a – a file that had an earlier date, or no date at all, but . . . only on my personal computer." (Tr. 100)

Applicant did not recall having a membership to a specific adult website, or visiting that specific website on his personal computer; that website was listed in GE 4 as having been discovered on his work computer. He said it was possible that the company's firewall let some inappropriate e-mails through and he clicked on them by mistake, but deleted them quickly. He recalled asking company IT to "beef up" their e-mail firewall to stop such e-mails and access to such sites. (Tr. 69-70, 99)

Applicant no longer uses a company EHD to transfer professional files between home and work. He has a work laptop with a docking station at home that he uses instead. He does not keep work or proprietary files on his personal computer. (Tr. 109-110)

Applicant has not been in counseling or therapy with respect to pornography. (Tr. 101) He continues to view pornography at home, including occasionally with his wife. (Tr. 91, 100)

Applicant believes that other employees of company 1 had professional access to administrative passwords, as he did, and "easily could access any [company 1] laptop or tablet and insert files onto that computing equipment." (AE A at ¶¶ 69-71; Tr. 45-47) He believes that company 1 "either invented any 'evidence' it claimed that it had, or, while I

was away from my desk, someone connected that personal [EHD] to the tablet and uploaded pornographic images from that personally owned external drive to the tablet." (AE A at ¶ 72) He believes that the real reason he was terminated was "because I had called out several instances of unethical behavior and business practices in the company." (AE A at ¶ 77)

On his September 2018 SCA, Applicant disclosed that he had been fired from company 1 for "alleged misuse of computer" and "I was told that pornographic files had been found on computer equipment in my possession." He also noted that this was shortly after he had filed formal complaints about another employee for sexual harassment of female employees "and lying to me about statements made by my staff." (GE 1 at 16, 17)

Applicant answered "No" to the following question on his SCA concerning unauthorized or unlawful use of information technology systems:

> **In the last seven (7) years** have you introduced, removed, or used hardware, software, or media in connection with any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines, or regulations or attempted any of the above? (GE 1 at 57)

Applicant's July 2019 background interview summary reflects that he was confronted with apparent evidence, through an interview with a coworker, of the fact that an investigation of Applicant's laptop found pornography linked to Applicant's username, password, and times and dates when he was logged in to the computer. (GE 2 at 2) The coworker is not identified and no specifics are provided, let alone documented, in GE 2. In the interview, Applicant denied any knowledge of the images. (GE 2 at 2) The remainder of Applicant's background interview largely concerns the sexual harassment allegations against Mr. C and Applicant's efforts to bring them to light; the May 2017 meeting with company officials that led to Applicant's termination; Applicant's assumption that Mr. C had something to do with transferring pornographic files onto Applicant's computer, and Applicant's discussion of his affair with S. (GE 2 at 2)

Work and Character References

J testified both as a character witness and a fact witness for Applicant. He has been a lawyer for almost 40 years, with about 17-18 years as general counsel for various defense contractors. He was general counsel for company 1 from 2004 to February 2010, when Applicant was there, and has known him since then. (Tr. 124-126, 137) J is now in private practice. (He was also Applicant's original counsel in this case, and filed Applicant's answer to the SOR, though he did not testify in that capacity). (Tr. 142-143)

As an in-house general counsel, J handled many company investigations of pornography on company computers. As such, J in his testimony took issue with company 1's handing of the investigation in this case. He testified that such investigations are typically discovered and investigated by HR and not by the legal department, though the

legal department would review the findings. (Tr. 127-128, 133-134) He also believes that company 1's legal department should have considered recusing itself from the investigation because the subject of the investigation was a senior company officer, as were others potentially involved. (Tr. 135) J also questioned the findings of the report, that there was evidence of pornography on work computers and any download of such materials during work hours, to support the conclusions in GE 4 that such conduct was established. (Tr. 135-136)

J acknowledged, however, that if it were confirmed that pornography was found on an employee's work computer, it was best practice, even "essential," to escort that employee from the building immediately and place the employee on either paid or unpaid leave. (Tr. 128) He also said where there was reasonable basis to believe such employee misconduct had taken place, "it's not a high bar." (Tr. 128)

J described Applicant as a brilliant intellectual, with both an engineering background and a "common sense" notion of how a business runs. (Tr. 138-139) He said Applicant has impeccable moral character, and an excellent sense of ethics, including as company 1's chief ethics officer. He is highly trustworthy and warrants being granted clearance eligibility. (Tr. 140-141, 145-146) Prior to his legal representation of Applicant, J was not aware of Applicant's sexual relationship with a subordinate employee. J has never put false information into an investigative report, nor would he ever do so. (Tr. 143-144)

Mr. M is a retired U.S. Navy captain and naval aviator, and a former employee of company 1. He was a company vice president who reported directly to Applicant. They had daily interaction, and often travelled together for work. They worked together for several months, about five years ago. They had met previously when Mr. M ran another company. (Tr. 115-119)

Mr. M was with Applicant the day Applicant was escorted out of the building. Mr. M heard days later that this happened because pornography had been found on a company laptop, "which struck me as really weird for a guy like [Applicant] who is smart as heck to do something so stupid, but he was gone, so I just let it go at that." (Tr. 120) Mr. M left company 1 about two months after Applicant was terminated. (Tr. 120)

Mr. M regards Applicant as someone of the highest intellect, one of the "top five" people in terms of intellect that he has met in 40 years of professional and military experience. He testified to Applicant's intelligence and "flawless" character, and attested that his judgment and trustworthiness were "beyond reproach." He was not aware of Applicant's relationship with S at the time it was occurring (Mr. M also was not working there at the time). (Tr. 117-119) Mr. M regards Applicant as a great American and an intellectual asset to the country. The fact that he may have had "something stupid on his computer is completely out of character." (Tr. 121-122)

Mr. M also testified that he was aware of a sexual harassment claim made against Mr. C by a woman who worked for Mr. M. Mr. M directed that she should report the matter to HR. He also reported it to Applicant. (Tr. 116)

Policies

The U.S. Supreme Court has recognized the substantial discretion the Executive Branch has in regulating access to information pertaining to national security, emphasizing that "no one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988). 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 required to be considered 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, these guidelines are applied in conjunction with the factors listed in the adjudicative process. The administrative judge's overall 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." In reaching this decision, I have drawn only those conclusions that are reasonable, logical, and based on the evidence contained in the record. 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 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 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. Section 7 of EO 10865 provides that 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

In May 2017, Applicant's employer conducted an investigation into his workplace conduct, including a romantic relationship with a subordinate employee in Applicant's chain of command, and the company's discovery of an extensive collection of pornography on Applicant's company computer systems.

Applicant acknowledged that he had a sexual relationship with S for several months in 2012, and acknowledged he later had an interest in renewing the relationship and taking it public, though this did not come to pass. He testified that company officials knew of the relationship in 2013, after it had ended. He said he was verbally reprimanded, but also subsequently promoted. GE 4 indicates that the affair came to light in 2017 when the subordinate employee raised concerns about working for Applicant, given their prior involvement. Both may well be true. While there was no company policy against the relationship, it was included as part of the company's rationale for terminating him because he did not report the relationship, and because it "set the wrong example and tone at the top" and potentially exposed the company to "significant legal and reputational risk" including possible claims of sexual harassment, a hostile workplace, and real or perceived favoritism. The relationship and interaction with S is long over, he expressed regret for it, and he has since remarried and moved across the country.

The allegations regarding the discovery of pornography on Applicant's company computers are more complex, largely since he not only does not admit it, but largely believes it to be fabricated in an attempt to get him fired (which worked, if that is what happened). Applicant acknowledges that he was terminated, but steadfastly and repeatedly denies that he knowingly and deliberately accessed, viewed, transferred, or stored any pornographic materials, images, or videos on any company computer system. He said he was not even aware of any inadvertent transfer, though he acknowledges that this is at least possible, given his history of viewing and storing pornography at home on his personal computer, since at least 2011, and because he transferred work files to and from his personal computer and his work tablet through a personal EHD. He denied e-mailing a list of pornographic movie files from his work e-mail account to his personal e-mail and denied having any "recent downloads" file. But he acknowledged that he may have maintained such a list on his personal computer. He denied being a member of a specific pornographic website.

Applicant repeatedly surmised, without corroboration, that his disputes with the company in general, and with Mr. C in particular, led to his termination. He indicated, at least in his affidavit, that others in the company had the knowledge and ability to install pornography on his company computer tablet or EHD, and might even have actually done so in an attempt to set him up and get him fired. At hearing, he did not go quite that far, saying only that he did not do so himself.

There are several problems with this. First, Applicant readily acknowledges a long history of accessing, viewing and storing pornography on his personal computer at home. Unless others at the company either knew this and used that information to set him up (which is not established), or were trying to set him up and looked at his personal EHD and got lucky by finding pornography (which is also not established), his acknowledged history of downloading pornography in his personal life at home makes it all the more likely that it was Applicant who was responsible for the pornography found on his work computer systems, regardless of how it got there. And it even makes it more likely than not that Applicant was viewing, accessing, and storing pornography at work and does not want to admit it. And if Applicant is to be fully believed, his uncorroborated theory leaves one to

wonder whether company officials had reason to know of his history of personal pornography use and used it against him at work, or, if they did not know, how they decided to put pornography on his work computers anyway. Further, if they went on pornographic websites to set him up and used company computers to do it, they would have had to violate their own company policy prohibiting accessing pornography.

In addition, company 1's findings and conclusions in GE 4 must be given some deference, as do the company's decisions about them. (ISCR Case No. 10-03886 at 3 (App. Bd. Apr. 26. 2012)). The Appeal Board has held that such deference extends to an employer's internal investigation. (ISCR Case No. 18-02592 at 4 (App. Bd. Jan, 6, 2021 (citing ISCR 18-00496 at 4-5 (App. Bd. Nov. 8, 2019)). I make this conclusion notwithstanding the fact that GE 4 contains an unexplained error as to the sequence and timing of events, in that Mr. F's initial discovery of pornography could not have taken place on May 2, 2017 if it led him to ask IT to take action on May 1, 2017.

Despite this unexplained discrepancy, GE 4 establishes that, following an investigation, company 1 found an extensive collection of pornography on Applicant's work computers. Much of the collection was years old even in 2017 but some (such as the "Recent downloads 4-8-17") suggest more recent activity. Given the extensive and quite specific evidence addressed in GE 4, and the fact that I am required to give that evidence some deference, that puts the burden on Applicant to disprove and mitigate it.

Moreover, the fact remains that Applicant was terminated for cause in May 2017 after an extensive collection of pornography was found on his work computer systems following a company investigation, as detailed in GE 4. As Applicant's own witness acknowledged, the company did not have a "high bar" to clear to find grounds for his immediate termination in the best interests of the company. Applicant has the burden of rebutting the record evidence supporting his termination for cause.

I must weigh Applicant's credibility against the documentary evidence supporting the SOR allegations. Once security concerns are established, Applicant has the burdens of production and persuasion in establishing sufficient mitigation to overcome the security concerns raised as to his clearance eligibility. With that backdrop, I now turn to analysis of these findings under the three guidelines alleged.

Guideline D: Sexual Behavior

AG ¶ 12 expresses the security concerns for sexual conduct:

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

(a) sexual behavior of a criminal nature, whether or not the individual has been prosecuted;

(b) a pattern of compulsive, self-destructive, or high-risk sexual behavior that the individual is unable to stop;

(c) sexual behavior that causes an individual to be vulnerable to coercion, exploitation, or duress; and

(d) sexual behavior of a public nature or that reflects lack of discretion or judgment.

The definition of sexual behavior under the Guideline D general concern "includes conduct occurring in person or via audio, visual, electronic, or written transmission." I find that viewing, accessing, and storing pornography satisfies this definition.

I find that AG ¶ 13(c) applies, as does AG ¶ 13(d), both as to the public nature of the behavior (on work computers) and since it reflects a lack of discretion or judgment. At the very least, particularly given his education and professional position as chief technology officer, Applicant exercised poor discretion and judgment in taking action (backing up work files he was working on at home, on a personal computer he used to access pornography), which conceivably led to the transfer of pornography onto his work computers. Applicant's sexual relationship with a subordinate is not alleged under Guideline D, so no disqualifying conditions apply to that circumstance.

Under AG ¶ 14, the following mitigating conditions are potentially applicable:

(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; and

(d) the sexual behavior is strictly private, consensual, and discreet.

Applicant has already felt the consequences of his behavior, in that he was terminated upon its discovery by his employer. His behavior no longer serves as a basis for coercion, exploitation or duress, and AG ¶ 14(c) applies. Applicant's use of pornography

was intended to be strictly private and discreet. AG ¶ 14(d) also applies.

The security concern with respect to Applicant's use of pornography is not the use itself, but rather the fact that an extensive collection of pornography was discovered on his work computers, leading to his termination. That circumstance suggests poor judgment and failure or unwillingness to comply with rules and regulations, particularly ones he had responsibility to follow in his high-level position. The evidence (GE 4) indicates that many of the videos and images were from 2010 to 2012, though there is also reference to "recent downloads" of pornography in April 2017, shortly before he was terminated. Even that evidence is now five years old. While his use was not infrequent, it also largely occurred during and after a period of separation and divorce as his second marriage was ending. Applicant has now remarried and begun a new life. His interest in pornography itself, in his personal life in more recent years, does not itself suggest a security concern. With respect to SOR ¶ 1.a, AG ¶ 14(b) applies.

Guideline M: Use of Information Technology

The security concerns about use of information technology are set forth 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 the question the willingness or ability to properly protect sensitive systems, networks, and 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 describes conditions that could raise a security concern and may be disqualifying. The following disqualifying conditions are potentially applicable:

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

The evidence of an extensive collection of pornography on Applicant's work computers, in violation of company policy establishes AG ¶ 40(e), as well as AG ¶ 40(f), as introduction of prohibited media, since company 1 specifically prohibited browsing pornographic sites and posting, sending, or acquiring sexually oriented material.

Under AG ¶ 41, the following mitigating conditions are potentially applicable:

> (a) so much time has elapsed since the behavior happened, or it happened under such unusual circumstances, that it is unlikely to recur and does not

cast doubt on the individual's reliability, trustworthiness, or good judgment;

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

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

AG ¶ 41(b) does not apply. The collection of pornography found on Applicant's company computers was extensive and therefore not minor. Applicant's misuse of an information technology system was serious because of the potential harm that can occur from accessing images from unapproved websites, such as pornographic websites. It can lead to inadvertent and unknowing insertion of a computer virus or malware on an information technology system. Applicant, as the chief strategy and technology officer for company 1 at the time, would know this better than many people.

Even if the presence of the pornography on his company computers systems *were* inadvertent, it stands to reason that it got there during a transfer (or transfers) of data between Applicant's home and work computers, through his personal EHD. In his position as chief technology officer, Applicant should have known that this might happen. He also made no attempt to bring such information to the attention of appropriate personnel (of which, in his position, he was one). AG ¶ 41(c) does not apply.

AG ¶ 41(a) has some application due to the age of the conduct, and the fact that much of the use here took place, albeit over a long period, when Applicant was experiencing marital instability. However, as noted above under Guideline D, the current security concern is not so much the pornography use itself, but its extensive presence on Applicant's company computers, in violation of a policy that he not only knew about but helped to draft, as the company's chief technology officer.

In contrast to his relationship with S, Applicant does not acknowledge any wrongdoing with respect to the pornography found on his company computers. Indeed, much of his defense hinges on his belief that he was essentially set up by people at the company seeking to remove him. As noted, once security concerns are established, it is Applicant's burden to provide sufficient evidence to mitigate those concerns. In order to do that here, he must overcome GE 4, and company 1's reliance on it in terminating him for cause. Further, in order for AG ¶ 41(a) to fully apply, Applicant must show that the circumstances that led to his termination were unusual, are unlikely to recur, and no longer cast doubt on his individual's reliability, trustworthiness, or good judgment. I cannot conclude that to be the case. Applicant tellingly does not acknowledge wrongdoing with respect to his computer conduct in the face of credible, detailed evidence from company 1 detailing their findings and conclusions that he engaged in the conduct. AG ¶ 41(a) does not fully apply.

Guideline E, Personal Conduct

AG ¶ 15 expresses the security concerns 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. . . .

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

> (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;
> >
> > (3) a pattern of dishonesty or rule violations; and
> >
> > (4) evidence of significant misuse of Government or other employer's time or resources; 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's relationship with S was not alleged under Guideline D, but is alleged under Guideline E. While there was no company policy against the relationship, it was part of the company's rationale for terminating him because he did not report it and because it "set the wrong example and tone at the top," potentially exposing the company to "significant legal and reputational risk" including possible claims of sexual harassment, a hostile workplace, and real or perceived favoritism. Applicant's relationship with S, a subordinate employee within his area of responsibility, satisfies AG ¶ 16(2) (any disruptive or inappropriate behavior); AG ¶ 16(e)(1); as well as the general security concern in AG ¶ 15 (questionable judgment).

The evidence of pornography on Applicant's work computer systems, as cross-alleged under Guideline E, satisfies multiple disqualifying conditions, including AG ¶

16(d)(2) (any inappropriate behavior); AG ¶16(d)(3) (pattern of rule violations); AG ¶16(d)(4) (evidence of significant misuse of employer's time or resources); AG ¶ 16(e)(1); as well as the general security concern in AG ¶ 15 (questionable judgment).

AG ¶ 17 sets forth potentially applicable mitigating conditions under Guideline E:

> (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;
>
> (e) the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress; and
>
> (f) the information was unsubstantiated or from a source of questionable reliability.

As to AG ¶17(f), Applicant argues that GE 4 was of questionable reliability, as in his view it was not created through best practices, is insufficiently supported, and contains an unexplained date discrepancy. However, as noted, I am required to give significant deference to an employer's actions, and, as J noted in his testimony, when pornography is found on an employer's work computer, it is not a "high bar" to conclude that immediate termination is appropriate. AG ¶ 17(f) does not apply.

As to the pornography, AG ¶ 17(e) applies under the same rationale as AG ¶ 14(c) above under Guideline D. Applicant has already felt the consequences of his behavior, in that he was terminated upon its discovery by his employer. His behavior no longer serves as a basis for coercion, exploitation or duress. As to the relationship with S, AG ¶ 17(e) also applies. The relationship is long over, he expressed regret for it, and he has since remarried and moved across the country.

AG ¶¶ 17(c) and 17(d) can be addressed together. As discussed, I am required to give deference to the employer's actions and rationale for terminating Applicant, and do so. Once a security concern is established, it is Applicant's burden of production and persuasion to establish mitigation.

To overcome GE 4 requires me to rely heavily on Applicant's credibility, and to lend significant credence to his version of events. To believe that, I have to accept not only that his employer wanted to terminate him but that they manufactured evidence of pornography on his company computers as grounds by which to do so. Such evidence is uncorroborated. Applicant's testimony, and that of his witnesses, is insufficient in this

regard to overcome the company's conclusions. In short, I find it very difficult to believe that company 1 manufactured evidence against Applicant, and in doing so, exploited a vice that Applicant happened to engage in privately. It is far more likely that, the company's report is accurate in many particulars – none of which Applicant has admitted. In short, I do not find Applicant's explanations credible, when balanced against the Government's evidence, particularly when he has a long history of viewing pornography in his private life.

As noted, the events in this case are now several years old. However, what is most concerning here is that Applicant has not acknowledged any wrongdoing with respect to the pornography allegation, in the face of quite strong evidence from company 1. This weighs against its mitigation, because his explanations are speculative, not sufficiently corroborated, and not credible. His position continues to cast doubt on his judgment, trustworthiness, and reliability. I therefore cannot conclude that AG ¶¶ 17(c) and 17(d) fully apply.

Whole-Person Concept

In assessing the whole person, the administrative judge must consider the totality of an applicant's conduct and all relevant circumstances in light of the nine adjudicative process factors in AG ¶ 2(d). The analyses under Guidelines D, M and E 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.

The security concern at this point is not the pornography. The security concern here is Applicant's judgment, his violation of company policy, and the fact that, in the face of strong evidence of his misconduct, his failure to acknowledge wrongdoing with respect to the pornography.

Applicant is a highly educated, very intelligent professional, working at a senior level in a technical field. He has a long career in the defense industry with a clearance, as evidenced not only by his own evidence and testimony but also his witnesses. I gave due consideration to this evidence in mitigation and under the whole-person concept.

As noted, it is Applicant's burden to overcome the security concerns once established. The conduct at issue here is quite dated, as it is now about five years old. But I am troubled most by Applicant's attempts to avoid blame for his conduct, and to seek to attach blame to others, in a highly speculative and self-serving manner, with insufficient corroborating evidence. His position is not credible and, in the face of reasonable, substantial, and specific evidence that he engaged in the conduct. this makes it difficult to conclude that circumstances have changed, or that Applicant would appropriately accept blame for future actions, rather than attempting to shift it to others, in a future situation of security significance.

The security clearance adjudication involves an evaluation of an applicant's judgment, reliability, and trustworthiness in light of the security guidelines in the Directive. *See* ISCR Case No. 09-02160 (App. Bd. Jun. 21, 2010). It is well settled that once a

concern arises regarding an applicant's security clearance eligibility, there is a strong presumption against the grant or renewal of a security clearance. *See Dorfmont v. Brown*, 913 F. 2d 1399, 1401 (9th Cir. 1990). For the reasons noted above, I am unable to conclude that it is clearly consistent with the national interest to grant or continue security clearance eligibility for Applicant.

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 D:	FOR APPLICANT
Subparagraph 1.a:	For Applicant
Paragraph 2, Guideline M:	AGAINST APPLICANT
Subparagraph 2.a:	Against Applicant
Paragraph 3, Guideline E:	AGAINST APPLICANT
Subparagraph 3.a:	For Applicant
Subparagraph 3.b:	Against Applicant

Conclusion

In light of all of the circumstances, it is not clearly consistent with the interests of national security to grant Applicant eligibility for a security clearance.

_____
Braden M. Murphy
Administrative Judge