DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 21-00528
	)	
Applicant for Security Clearance	)	

Appearances

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

11/15/2023

_____

Decision

_____

BENSON, Pamela C., Administrative Judge:

Applicant failed to mitigate the security concerns under Guidelines M (Use of Information Technology), K (Handling Protected Information), and E (Personal Conduct). National security eligibility for access to classified information is denied.

Statement of the Case

On June 3, 2019, Applicant submitted a security clearance application (SCA). On January 18, 2023, the Defense Counterintelligence Security Agency (DCSA) Consolidated Adjudication Services (CAS) issued Applicant a Statement of Reasons (SOR), detailing security concerns under Guidelines M (Use of Information Technology), K (Handling Protected Information), and E (Personal Conduct). The action was taken 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) effective within the DOD on June 8, 2017.

Applicant answered the SOR in February 2023. He denied SOR ¶¶ 1.a, 1.b, 1.d through 1.h, 2.a, 3.b, and 3.d. He admitted SOR ¶¶ 1.c, 3.a, and 3.c. He requested a

hearing before a Defense Office of Hearings and Appeals (DOHA) administrative judge. On May 5, 2023, the case was assigned to me. On July 18, 2023, the DOHA issued a notice of hearing, setting the hearing for August 8, 2023.

The Government called a witness and offered Government Exhibits (GE) 1 through 6 into evidence. Applicant offered Applicant Exhibits (AE) A through G into evidence. All documents were admitted into evidence without objection. Applicant testified and also had a witness testify on his behalf. DOHA received the hearing transcript (Tr.) on August 15, 2023.

Findings of Fact

Having thoroughly considered the evidence in the record, I make the following findings of fact: Applicant is 51 years old. He enlisted in the Marine Corps in August 1990. He served in Desert Storm, Desert Shield, Operation Restore Hope, 31st Marine Expeditionary Unit (MEU) out of Okinawa, Japan, and on two sea service deployments throughout Southwest Asia. He earned a master's degree in 2007 from the Naval Postgraduate School in information technology management (ITM). He retired with an honorable discharge in July 2011 at the rank of staff sergeant. His decorations include the Meritorious Service Medal, Navy Commendation Medal, and three Navy Achievement Medals. He has an extensive background in IT and various certifications. Applicant was married in 1994 and subsequently divorced in 2018. He has an adult daughter, and a son, age 17. (Tr. 12-13, 23-25; GE 1, GE 2)

Applicant was hired in February 2014 by a government contractor as an operations manager. One of his responsibilities was to ensure that the company's IT operations ran smoothly. He held a DOD security clearance in this position. Under Guideline M (Use of Information Technology), SOR ¶ 1.a alleges that Applicant, while employed in this position and without the chief executive officer's (CEO) approval, obtained and utilized access to his employer's network drives, which contained the co-owners' personal information, as well as corporate sensitive information. (Tr. 23, 25-29; GE 4)

Applicant testified at the hearing that he had asked the co-owner (minority owner) of the company for system administrator access through an email communication, with the CEO copied on the email. In about June 2014, he was granted system administrator access in order to perform a network assessment. He admitted that with administrator access he had admittance to the owners' personal information and any company proprietary information that was saved on any of the drives on the network. He denied this allegation in his SOR Answer because he did not use or take any proprietary or sensitive information. Applicant also adamantly denied in his SOR Answer ever having system administrator access, which would have prevented him from doing some of the activities alleged in the SOR. This information contradicts his testimony. (Tr. 30-31, 51-52)

SOR ¶ 1.b alleges that Applicant, without being tasked to do so, gave an outside vendor and personal friend/acquaintance, access to his employer's network and allowed the vendor to install hardware/software devices on the network without prior approval. He did not obtain a nondisclosure agreement (NDA) from the vendor before giving the vendor access to sensitive company data.

In June 2014, Applicant hired vendor (A to come to the business where the vender installed software and hardware (Infoblox) to access the network to ensure cyber compliance and to perform network hardening, or the testing of vulnerabilities on the company's hard drives. Applicant was familiar with the person who worked for the software company, but not the vendor who used the software. After the vendor performed these services, Applicant admitted the CEO claimed that he had not been given authorization to have a vendor perform specific tasks during the network assessment. He stated that he had been clear during weekly work meetings of his intent to hire vendor A to access the company's network. He was present with the vendor the entire time they were on location performing these tasks. The vendor tested for vulnerabilities across the network and provided recommendations on how to harden the network. He was not aware that he was supposed to obtain an NDA from the vendor since he thought NDAs were only needed in business development. Applicant admitted he used the system administrator status he was granted so the vendor could perform these tests. He testified that he held the system administrator rights for about two weeks in June 2014. (Tr. 32-36, 50-52; GE 4)

A government witness, Mr. Z, with 31 years of IT experience and who also provided IT services to the federal contractor through his company, testified that a few weeks before Applicant resigned from his employment, Mr. Z was tasked with reviewing and monitoring the government contractor's network to determine if any company documents were lost or if any data was transferred from the company's network. Mr. Z testified that he managed all the rights, permissions, and access to data on the company's network. He did not grant system administrator privileges to Applicant, but in May 2014, he did grant vendor A full access through a temporary system administrator account. Applicant was also able to have system administrator access via the temporary account that was to be used only by the vendor. He stated that Applicant used the temporary account access privileges from May 2014 until late September 2014, when an employee reported that Applicant had complete domain administrator privileges because Applicant had given him the account access password. Mr. Z testified that the security manager immediately requested that he remove Applicant's access through the temporary account created for the vendor. (Tr. 18, 97-99, 101-103, 105-107; GE 2, 4)

SOR ¶ 1.c alleges that on January 14, 2015, Applicant downloaded his employer's proprietary information, sensitive personal information regarding the employer's owners, and project data related to one or more government contracts. He saved approximately 7 GB of data to a personal Dropbox and then deleted evidence of the activity from his work laptop.

Applicant testified this event occurred about a month before he left this place of employment. He stated that he installed a Dropbox account due to employees having difficulty obtaining information from the company drives. This Dropbox allowed project employees access to information while there were at their customer worksites. The information he placed in the Dropbox was necessary for the employees to perform their job duties, and he said the Dropbox was in full compliance with IT rules and regulations. He did not recall asking for permission to set up the Dropbox account but stated he had provided notice during the weekly meetings that he was going to do so. He started moving data into the Dropbox, which he claimed was a secure environment, using his work e-mail. He worked out of the conference room on a regular basis and sometimes turned off the lights to take advantage of the natural lighting. As soon as the CEO found out that he had completed this task, she got extremely upset, and he immediately deleted the information he had placed into the Dropbox. (Tr. 36-45, 62-64; GE 2)

Mr. Z testified that the night of January 14, 2015, just before Applicant departed from his employment, he was accessing files from the company's server at 4:20 p.m. The forensic evidence showed that about 7 GB of data was transferred onto Applicant's laptop in his Dropbox account. Mr. Z stated that the Dropbox was not a secure or proper way to handle the transference of sensitive information. The office video camera footage showed that at 6:26 p.m., Applicant turned off the lights in the conference room while waiting for the data to migrate. At 7:04 p.m., Applicant deleted the Dropbox content from his laptop with encryption to prevent detection. Security video footage also showed that Applicant then turned on the lights, activated the building's security alarm, and exited the building with his personal belongings in hand. Based on the forensic evidence found by Mr. Z during an examination of Applicant's work laptop, the CEO filed an incident report against Applicant. She accused Applicant of downloading company proprietary information and sensitive personal information concerning the owners of the company, and project data related to one or more government contracts that was possibly considered Controlled Technical Information. On this day, Applicant moved the data into a personal Dropbox account on his work laptop using his personal email, and then he deleted the trail from his laptop that same evening with the use of File Sanitizer, which was used to permanently delete files. Less than a week after this incident, Applicant submitted his letter of resignation to the company. The detailed analysis of forensic data recovered from Applicant's laptop was provided to the Defense Security Service and the FBI. (Tr. 107-112; GE 2, 3, 4)

Due to this incident, in April 2015, the security manager of the government contractor contacted their customer on a government contract to self-report a security incident concerning their former employee. The security manager informed their customer that Applicant had downloaded sensitive information regarding the contract, and requested further direction from the customer. (GE 4)

SOR ¶ 1.d alleges that Applicant violated his employer's IT policies when he used his work laptop to download or access pornographic material. Applicant testified that he was not aware that he had accessed pornography on his work laptop, but he takes accountability for this transgression. "I'm not saying I didn't do it. I'm just not

aware of it." He testified that he would never download porn but he could have accessed porn on his work laptop. He was aware that he should generally not access pornography on a work laptop, but he was not aware of any specific rule or policy that prohibited such conduct. He was not aware that porn sites were notorious for having viruses or malware. (Tr. 46, 77-78; GE 4)

SOR ¶ 1.e alleges that Applicant "enabled" or tampered with "HP Protect" security software on his laptop in violation of company policy. Applicant stated that he did use HP Protect to wipe the work computer when he was departing his employment in February 2015, which he thought was an acceptable practice at most companies. He denied installing HP Protect on his work computer because he believed it was already preloaded onto his work computer. He did not admit to wiping his computer clean on more than one occasion, but he did admit he did so at the end of his employment. (Tr. 36-45, 47-49; 62-64; GE 2, 4)

Mr. Z testified that wiping a computer clean is a red flag for IT professionals that someone is trying to hide something on their computer. Wiping a computer before departing a place of employment is also not a common practice within the industry. He testified that a standard user should not have access to do a factory reset of the work computer unless they had administrator rights. When a laptop is returned by an employee, all that is needed is to wipe out the user's profile. There is no need to initiate a complete wipe of the computer. Mr. Z said that Applicant had completed a previous wipe to his work laptop in either July or August 2014, in addition to the wipe he performed in February 2015, based on his forensic analysis. Mr. Z was able to recover most of the deleted data on Applicant's laptop by using R-Studio, and other applications in his forensic examination. He determined that Applicant had been able to do many activities that a standard IT user would not be able to do. (Tr. 108-117; GE 4)

SOR ¶ 1.f alleges that Applicant created multiple usernames and passwords without IT or CEO permission in violation of company policy. Applicant stated this incident stemmed from the time he hired a vendor to perform system checks and vulnerabilities on the company's network. He created multiple usernames and passwords so that the system screenings could be performed. Another employee reported to the security manager in September 2014 that Applicant had given him the system administration password. The security manager contacted Mr. Z and requested that Applicant's system administrator access be removed immediately. When Applicant was questioned about this incident, he stated; "I don't really understand the context, so it's hard for me to say." (Tr. 50-52; GE 4, 5)

SOR ¶ 1.g alleges that Applicant installed unauthorized software on his company laptop in violation of company policy. Department Counsel acknowledged this SOR allegation somewhat overlapped with the allegation of Applicant installing or using HP Protect software. Applicant stated in his SOR response "I did not utilize, nor was I afforded system administration or network administration right in any capacity of my job." This sentiment is repeated several times in his SOR Answer. His testimony indicated he was granted system administrator privileges for approximately two weeks

in June 2014 by the minority owner. Applicant explained previously that the HP Protect software was already preloaded on his work computer, but the IT provider, Mr. Z, testified that he deleted all applications of HP Protect from all of the work laptops provided to government contractor employees. When I specifically asked Applicant if he had downloaded HP Protect, which was used to wipe his laptop, his response was; "No, not that I'm aware of." He denied knowledge of the File Shredder on his laptop, and explained that the Dropbox account was not software but was actually "a link to go to the internet" in order to interface with an encrypted site, like a cloud. (Tr. 47, 52-54, 56-57; SOR Answer; GE 4)

Mr. Z testified that the federal contractor did not utilize Dropbox. He stated that government contractors are not permitted to store any information on the cloud unless it is an approved government cloud, such as DOD SAFE, for instance. He also pointed out that if an employee needed Dropbox, they would use their work email address and create the account. Applicant did not use his work email address. Applicant used his personal account when using Dropbox on his computer. Mr. Z stated that the analysis of the Dropbox not only showed the contractor's data was stored there, but also showed data Applicant had taken from a previous employer. Mr. Z stated, "so, we see a pattern here." (Tr. 117-122; GE 4)

SOR ¶ 1.h alleges that Applicant disabled or failed to run virus protection on his work laptop, which resulted in malware virus infestation of his local profile. He denied this allegation in his Answer and again during his testimony. When questioned about his access to porn websites to view pornography, I asked Applicant whether it was common knowledge in the IT industry that many of these porn websites contained viruses or malware. Applicant answered that he was not aware of this information. (Tr. 54-55, 77-78; SOR Answer; GE 4)

Mr. Z logged into Applicant's work laptop and discovered that there was not an active virus defense application installed. A full scan of the computer revealed Trojan viruses and malware in the local profile used by Applicant. Mr. Z had to have the viruses and malware removed before a detailed analysis of Applicant's laptop could be completed. Mr. Z also noted that accessing pornographic websites could have contributed to the viruses and malware on the laptop. (GE 4)

Applicant departed employment with the federal contractor in February 2015 and started a franchise. He testified that the franchise did not interfere or overlap with the business of his former employer. He operated the franchise for five years while he also worked concurrently as a sales director for another company. Since 2018, Applicant has served as a vice president of his current company, and he is requesting a DOD security clearance be granted so he can perform specific job duties. (GE 1; Tr. 12-13, 22-23; SOR Answer)

Paragraph 2 of the SOR alleged Guideline K (Handling Protected information) security concerns, and it cross-alleged SOR ¶¶ 1.a-1.c. Applicant denied that he

mishandled protected information in any way. (SOR ¶ 2.a) Paragraph 3 of the SOR alleged Guideline E (Personal Conduct) security concerns, as follows:

SOR ¶ 3.a alleges that in approximately August 2014, Applicant refused a direct order from the CEO to lay off an employee. Applicant admitted this information in his Answer. Instead of laying off the employee, he stated that the CEO wanted him to fire the female employee for a dress code violation, specifically, for a skirt that was too short. Applicant determined that this employee was not in violation of company policy and refused to fire the employee. A meeting followed, and the CEO again asked Applicant to fire the employee. Applicant stated that he refused because the female was not his employee and because he believed that both owners of the company were also in violation of the dress code policy. Applicant denied that he had a close relationship with this employee, but he did acknowledge she was hired to work for his franchise after he left the government contractor. The CEO reported that Applicant was asked to lay off the employee due to lack of contract work, and he refused. (Tr. 64-69; GE 5)

SOR ¶ 3.b alleges that in approximately August 2014, Applicant informed the company's security officer that he already had possession of all of his employer's data. Applicant denied this information. He stated in his Answer that any data that he maintained was for the normal performance of his employment duties. He testified that because he did not have system administrative rights, he denied that he had "full" access to all of the company's data. (Tr. 69-70; GE 5)

SOR ¶ 3.c alleges that while Applicant was the sole administer of his employer's LinkedIn account, he allowed, or caused, the employer's page to be changed or redirect visitors to Applicant's new startup company, rather than the federal contractor. Applicant admitted setting up his employer's LinkedIn account. After his departure, he was not aware he was the sole person who retained rights to the LinkedIn account. Once the human resources director contacted him about this matter, he immediately provided access and privileges to his previous employer. His testimony was that this was a misunderstanding and in no way intentional. (Tr. 70-72; GE 6)

SOR ¶ 3.d cross-alleged all of the information cited under Paragraphs 1 and 2. Applicant denied this information.

Character Evidence

Applicant called a former colleague who had worked with him while employed by the same government contractor. The individual said he felt compelled to testify on behalf of Applicant because after he left this same employer in early 2016, the company's CEO also falsely charged him with many of the same accusations they made about Applicant after his departure in February 2015. The witness believed these were company tactics to prevent employees from competing with the company's business. He clarified that his role in this company was business development, and he was not involved in IT. He also admitted that he continued to develop business after leaving this employment, and the federal contractor was successful in preventing him

from pursuing business with a contact he had developed. The witness also testified that he has worked on many projects with Applicant, and Applicant's business and personal actions were always beyond reproach. He recommended that Applicant be granted a DOD security clearance. (Tr. 82-93; AE F, G)

Applicant also provided character-reference letters from a previous employee, supervisor, and the president of the federal contractor that currently employs Applicant. The general sense of the character evidence is that he is diligent, professional, productive, reliable, and trustworthy. Applicant continues to provide important contributions to warfighters' mission. His character statements support reinstatement of his security clearance. (AE C, D, E)

Policies

When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the AG. In addition to brief introductory explanations for each guideline, the AG list potentially disqualifying conditions and mitigating conditions, which are 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, these guidelines are applied in conjunction with the factors listed in the adjudicative process. The administrative judge's overarching adjudicative goal is a fair, impartial, and commonsense decision. According to AG ¶ 2(c), 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. Likewise, I have avoided drawing inferences grounded on mere speculation or conjecture.

Under Directive ¶ E3.1.14, the Government must present evidence to establish controverted facts alleged in the SOR. Directive ¶ E3.1.15 an "applicant is responsible for presenting witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by applicant or proven by Department Counsel, and has the ultimate burden of persuasion as to obtaining 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 an applicant may deliberately or inadvertently fail to safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation as to 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

Guideline K: Handling Protected Information, and Guideline M: Use of Information Technology

Due to the overlap in security concerns, disqualifying conditions, and mitigating conditions in the context of Applicant's conduct with IT systems and the handling of protected information while employed by a government contractor, these two guidelines are discussed together, below.

The security concern under Guideline K is set out in AG ¶ 33 as follows:

> Deliberate or negligent failure to comply with rules and regulations for handling protected information which includes classified and other sensitive government information, and proprietary information raises doubt about an individual's trustworthiness, judgment, reliability, or willingness and ability to safeguard such information, and is a serious security concern.

The security concern under Guideline M relating to the use of information technology is set out in AG ¶ 39:

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

The following conditions under Guideline K, AG ¶ 34, are potentially disqualifying:

> (b) collecting or storing protected information in any unauthorized location;
>
> (c) loading, drafting, editing, modifying, storing, transmitting, or otherwise handling protected information, including images, on any unauthorized equipment or medium; and
>
> (g) any failure to comply with rules for the protection of classified or sensitive information.

The following disqualifying conditions under under Guideline M, AG ¶ 40 are potentially applicable:

> (c) use of any information technology system to gain unauthorized access to another system or to a compartmented area within the same system;
>
> (d) downloading, storing, or transmitting classified, sensitive, proprietary, or other protected information on or to any unauthorized information technology system;
>
> (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 SOR alleges and the employer's investigative report shows that Applicant had access to network drives and data that he was not authorized to have access to, he downloaded thousands of electronic files, to include proprietary information files, from his former employer's network without authorization, saving it to a personal Dropbox, and then deleting evidence of this activity, and he installed and used software on his work laptop without authorization. The above disqualifying conditions under Guidelines K and M have been established.

AG ¶ 35 of Guideline K contains three mitigating conditions that have possible applicability to the facts of this case:

> (a) so much time has elapsed since the behavior, or it has happened 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 good judgment;

(c) the security violations were due to improper or inadequate training or unclear instructions; and

(d) the violation was inadvertent, it was promptly reported, there is no evidence of compromise, and it does not suggest a pattern.

The following mitigating conditions under Guideline M, AG ¶ 41 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;

(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.

The Appeal Board gives deference to a company's findings and conclusions in its security investigations. *See*, e.g., ISCR Case No. 15-08385 at 4 (App. Bd. May 23, 2018) ("[B]ecause of the unique position of employers as actual administrators of classified programs and the degree of knowledge possessed by them in any particular case, their determinations and characterizations regarding security violations are entitled to considerable deference, and should not be discounted or contradicted without a cogent explanation.").

Applicant repeatedly denied in his SOR Answer that he had systems administrator access to the company's network, and without this access, he would not have had the ability to perform several of the alleged IT operations, such as downloading, storing, or transmitting classified, sensitive, proprietary, or other protected information that he did not have authorization to access, or be able to install other software. At the hearing, however, Applicant admitted he did have this access for about two weeks in June 2014, while he was working with vendor A to conduct an analysis of the company's network. Mr. Z also testified that he had granted temporary complete domain administrator rights access to be used by the vendor, but he was later notified that Applicant had unauthorized access through this temporary account and Mr. Z was tasked with the immediate removal of his access in late September 2014. With the temporary administrator account Applicant had access to everything on the company network.

Applicant has made inconsistent statements about him having access to system administrative rights at his previous place of employment. He also stated that on January 14, 2015, just before he gave the CEO his resignation letter, he was working to move company data from the network to the Dropbox account. He claimed that he had set up an account under his work email, but Mr. Z stated the Dropbox account was actually Applicant's personal account. Applicant testified that when the CEO discovered the Dropbox account and after she let him know she was upset, he immediately deleted the data from the Dropbox account. However, the evidence showed that after Applicant had migrated 7 GB of the company's data into the Dropbox account on January 14, 2015, with the lights turned off, he then immediately deleted evidence of his activities before he left the work building. Understandably, an employee's downloading of a large number of files shortly before submitting his letter of resignation raises concerns. Applicant has extensive experience and knowledge in the IT field. I find that his actions that day were highly suspicious. Mr. Z's analysis of Applicant's laptop gave evidence that not only the company's data was discovered, but he also found proprietary data from Applicant's previous employer. The forensic evidence showed a pattern, and the employer's conclusions from the investigative findings of this case is given deference.

Applicant's total wipe of his work laptop is also concerning because it shows that he was trying to hide his past activities. There were applications that had been downloaded on the laptop that were not provided by the company. Mr. Z testified that it is not a common practice, as Applicant claimed, for an employee to do a total wipe of a laptop before turning it into the IT manager. He noted that a regular user would not have been able to conduct a factory reset of the laptop either. Mr. Z stated that in the IT industry, any individual who does a total wipe of their work computer immediately raises a red flag that the user was trying to hide their past activities. The fact that Applicant completed a wipe of his work computer on two occasions during his one-year tenure with the government contractor is troubling.

Applicant could not recall whether he accessed pornography on his work laptop, but he said that he would take responsibility for it. His statement that accessing pornography on his work laptop generally was a bad idea, but *he did not violate any company policy he was aware of* (emphasis added), is just not credible and undercuts the believability of his claim. His actions, and his continued denial of improper conduct despite his former employer's conflicting forensic data, continues to demonstrate that he is not trustworthy or reliable. None of the mitigating conditions listed in AG ¶ 35 and AG ¶ 41 are applicable.

Guideline E: Personal Conduct

AG ¶ 15 expresses 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

provide truthful and candid answers during national security investigative or adjudicative processes. …

The following disqualifying conditions under AG ¶ 16 are potentially applicable:

> (c) credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any single guideline, but which, when considered as a whole, supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the individual may not properly safeguard classified or sensitive information;
>
> (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:
>
> > (3) a pattern of dishonesty or rule violations; and
> >
> > (4) evidence of significant misuse of Government or other employer's time or resources.
>
> (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; and
>
> (f) violation of a written or recorded commitment made by the individual to the employer as a condition of employment.

The SOR alleges under Guideline E that Applicant refused a direct order to lay off an employee while employed with the government contractor; while Applicant was the sole administrator for his employer's LinkedIn account, he caused the employer's page to be changed and redirected visitors to his new company; and that Applicant told the security manager in August 2014 that he already had all of the government contractor's information.

In addition, three of the SOR allegations under Guideline M were cross-alleged under Guidelines K and E. Applicant's conduct could affect his personal and professional standing if it became known by his current or future employers and that fact creates a vulnerability to exploitation, manipulation, or duress by others. His violation of his employer's IT protection policies violated the commitment he made when he became employed, which was a condition of his employment. The above disqualifying conditions apply.

The guideline also includes conditions that could mitigate security concerns arising from personal conduct. The following mitigating conditions under AG ¶ 17 are potentially applicable:

> (c) the offense is so minor or so much time has passed, or the behavior is so infrequent, or 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 acknowledged the behavior and obtained counseling to change the behavior or taken other positive steps to alleviate the stressors, circumstances, or factors that contributed to untrustworthy, unreliable, or other inappropriate behavior, and such behavior is unlikely to recur; and
>
> (e) individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress.

The three individual SOR allegations under Guideline E; failure to follow direct order of the CEO to lay off an employee, his statement to the security officer that he already had all of the company's data already, and the problems associated with the company's LinkedIn account were not sufficiently corroborated during the hearing or in the evidence in the record. Applicant's explanations for these events were logical and reasoable. SOR ¶¶ 3.a, 3.b, and 3.c are concluded for Applicant.

The central theme of this case is Applicant's violation of IT and company policies concerning protected and sensitive data. These actions (SOR ¶¶ 1.a, 1.b, and 1.c) were also alleged under this Guideline. His demeanor and testimony lacked credibility, and the inconsistencies between his testimony and the other evidence in the record further undermined his credibility. His behavior could affect his personal, professional, and community standing. His conduct is disqualifying under this guideline for the same reasons that it is disqualifying under Guidelines M and K, as discussed above. None of the mitigating conditions apply.

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 circumstances. The administrative judge should consider the nine adjudicative process factors listed at AG ¶ 2(d):

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

Under AG ¶ 2(c), the ultimate determination of whether to grant eligibility for a security clearance must be an overall commonsense judgment based upon careful consideration of the guidelines and the whole-person concept. I considered the potentially disqualifying and mitigating conditions in light of all the facts and circumstances surrounding this case. This SOR highlights serious offenses that provide insight to Applicant's character and integrity. Applicant is not remorseful for his misconduct and some of his explanations are self-serving and implausable. He has established a pattern of unwillingness to follow rules, policies, and regulations. Despite that this misconduct occurred several years ago, the grave seriousness of the matter and security implications remain. I conclude that Applicant has not mitigated security concerns raised by his use of information technology, handling protected information, and personal conduct.

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 M:	AGAINST APPLICANT
Subparagraphs 1.a-1.h:	Against Applicant
Paragraph 2, Guideline K:	AGAINST APPLICANT
Subparagraph 2.a:	Against Applicant
Paragraph 3, Guideline E:	AGAINST APPLICANT
Subparagraphs 3.a, b, and c:	For Applicant

Subparagraph 3.d: Against Applicant

Conclusion

In light of all of the circumstances presented by the record in this case, it is not clearly consistent with the national security to grant Applicant's eligibility for a security clearance. Eligibility for access to classified information is denied.

Pamela C. Benson
Administrative Judge