DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 18-00557
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Bryan Olmos, Esq., Department Counsel
For Applicant: *Pro se*

02/19/2020

_____

Decision

_____

HEINY, Claude R., Administrative Judge:

Applicant contests the Department of Defense's (DoD) intent to deny his eligibility for a security clearance to work in the defense industry. He provided sufficient evidence in explanation and mitigation resolving the use of information technology and personal conduct security concerns. Eligibility for access to classified information is granted.

Statement of the Case

On June 15, 2018, the Department of Defense Consolidated Adjudications Facility (DoD CAF) issued a Statement of Reasons (SOR) to Applicant, detailing the security concerns under Guideline M, use of information technology, and Guideline E, personal conduct, under which it was unable to find it clearly consistent with the national interest to grant or continue security clearance eligibility for him.

The DoD CAF acted under Executive Order 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 for Determining Eligibility for Access to Classified Information* (AG) effective within the DoD on June 8, 2017.

On July 23, 2018, Applicant answered the SOR allegations and requested a hearing before an administrative judge from the Defense Office of Hearings and Appeals (DOHA). (SOR Response) On March 21, 2019, DOHA issued a Notice of Hearing scheduling a hearing that was conducted on April 11, 2019.

Eleven Government exhibits (Ex. 1 – 11) and one Applicant exhibit (Ex. A) were admitted into evidence without objection at the hearing. Applicant testified, as reflected in a transcript (Tr.) received on April 19, 2019, as did a government witness, Applicant's former employer, and a coworker.

Findings of Fact

In Applicant's SOR answer, he admitted he had been terminated in 2011 from his then employment for a computer-use violation (SOR ¶ 1.a). Applicant denied he violated his administrative privileges as a systems administrator between April 2012 and September 2014(SOR ¶ 1.b); denied he permanently disabled anti-intrusion software on his workstation(SOR ¶ 1.b.i.); denied placing his workstation in any elevated category groups within an active directory (SOR ¶ 1.b.ii.); denied modifying his system configuration to violate security requirements (SOR ¶ 1.b.iii.); and denied violating his access privileges by accessing websites with inappropriate content, or uploading images of women in violation of the Acceptable Use Policy (SOR ¶¶ 1.c and 1.c.i.). He admitted his access to classified information was suspended in March 2015 (SOR ¶ 1.d) for the alleged violations of administrative and access privileges, but he was told only that there had been "suspicious activity." He denied being involved in conduct of questionable judgment under Guideline E, personal conduct (SOR ¶¶ 2 and 2.a). He denied falsifying facts on his May 4, 2015 Electronic Questionnaires for Investigations Processing (e-QIP) when he stated he left his employment in August 2011 due to end of contract and was released from the contract under mutual agreement (SOR ¶ 2.b). He denied he had failed to disclose on his July 31, 2017 e-QIP the full extent of his August employment termination. (SOR ¶ 2.c). (Ex. 3, 4) After considering the pleading, exhibits, and transcript, I make the following findings of fact:

Applicant is a 45-year-old information technology (IT) support specialist who has worked for a defense contractor since June 2017 and seeks to obtain a security clearance. (Ex. 5) From May 1999 through August 2003, he honorably served in the U.S. Marine Corps. (Ex. 4) In July 2009, he married, and in June 2016, he divorced. (Ex. 4) He has two children, a son age 14 and a daughter age 11. (Ex. 4) His confidential clearance eligibility was granted in May 1999, and suspended in March 2015. (Ex. 4, 5)

On August 22, 2011, Applicant was terminated from his employment with a technology company when he plugged a hard drive into a government computer, which held inappropriate content. (Ex. 6) He stated,

> in August of 2011 there was a lapse of judgment and I made a mistake and it was an isolated incident. It was not malicious in nature and under no circumstance was it meant to be a security breach or anything that would endanger the government system. It was a simple lack of judgment which cost me employment. (Tr. 12)

Applicant explained that he provided IT support to friends not part of his government job. His barber gave him an external hard drive to check if it was functional because it would not boot up. (Tr. 99, SOR Response) Instead of waiting to take the hard drive home to test it, he plugged it into his work computer. When he discovered the contents of the hard drive, he immediately unplugged it, but his action was a security violation. He acknowledges his actions were shortsighted and thoughtless. (SOR Response) He says there was "no excuse or justification for [his] unethical act," but asserts this action was not characteristic of how he handled business before or after the incident. (SOR Response) He stated, "I do freely admit that it was an error, a lapse in judgment, and I did plug into a hard drive." (Tr. 83) This was his first offense at the company. (Tr. 84) He testified, "it was a lapse of judgment which I'm not running away from it. This was back in 2011, and since then, of course, I've mitigated that and I'm very mindful and very paranoid" about during security access. (Tr. 87) He asserts he was very candid about the incident during both his Office of Personnel Management (OPM) interviews. (Tr. 87)

The day after Applicant connected the hard drive, his violation was detected, and Applicant was told not to return to work. (SOR Response) When confronted by his employer, he acknowledged his mistake and did not make or offer any excuse for the incident. The company was in the midst of a contract extension and re-bid of the contract and he was told it was best that he be separated. (Tr. 86, SOR Response) He was told he would not be given a second chance because the contract was ending, and retaining him after the security incident might hurt the company's chance of obtaining the contract. (Tr. 87)

Applicant disclosed on his January 2012 e-QIP and again on his July 2017 e-QIP, that he had left his job in August 2011 by mutual agreement following allegations of misconduct. On both e-QIPs, he fully explained that he had plugged in a hard drive on his work computer to test it. He stated that his then employer's Network Operations Center (NOC) had discovered the incident. He indicated that his actions were a security violation and stated,

> My company was in the midst of recompete efforts with [a government agency]. This would look bad for my old employer's desire for recompete. It was decided that it would be best if I were [sic] removed from the contract for that reason. I was told it was a result of bad timing as opposed to the violation itself. I understood violation and my employment with [the company] ended. (Ex. 1, Ex. 4)

In Applicant's January 31, 2012, Declaration for Federal Employment to work as a contract systems administrator for the U.S. military, he answered "yes" to question 12 that asked if, during the previous five years, he had been fired from any job for any reason, quit after being told that he would be fired, or left by mutual agreement because of specific problems. He explained he left his previous employer after mutual agreement after he had plugged a personal external hard drive into his work computer. He stated the incident was deemed a security violation and, due to the timing of the incident, his employment ended. He explained the contract he was working on was ending and the company was in negotiations to bid on a new contract. (Ex. 2) He asserts he had no intention to be dishonest or have a lack of candor. (Tr. 88)

On Applicant's May 2015 e-QIP, he answered "no" to all employment questions concerning being fired, quitting after being told he would be fired, leaving by mutual agreement following allegations of misconduct or unsatisfactory performance, or having received a written warning, reprimand, suspension, or discipline for misconduct in the work place. (Ex. 3) He gave as the reason for his employment ending in August 2011, "End of contract. Released from Contract under mutual agreement." (Ex. 3)

When asked about it during his OPM interviews, he told the investigators that his answer was a mistake and he should have answered "yes" to the questions on the e-QIP. (Tr. 107) He asserts he was candid throughout the investigation, with the OPM investigators, and during his hearing, and he was not deceptive or malicious. (Tr. 178)

On Applicant's July 2017 e-QIP, he provided a long explanation for his termination. (Ex. 4) He fully explained that his employment ended because he had plugged a hard drive into his government computer, which was discovered by the NOC. He explained his employer said it would look bad as the company was competing for an extension of the contract, and it would be better if he was removed from the contract. (Ex. 4) The company did not create an unfavorable information file (UIF) on the incident. (Tr. 135) He is remorseful about the incident. (Tr. 189) Before his initial hiring as a contractor in support of the U.S. military, Applicant told his prospective employer what occurred at his previous employment. (Tr. 134) The company checked it out and, according to Applicant, his previous employer related the same information Applicant had provided. (Tr. 134) The contractor at JTFB would not have hired Applicant had his previous employer recommended he not be hired. (Tr. 136)

From April 2012 until September 2014, Applicant worked as a contractor in support of the U.S. military at an overseas government location. (Ex. 5) He was employed along with 17 or 18 other U.S. computer technicians; the prime contractor had an additional 24 to 25 U.S. computer technicians; and the host country had an equal number of technicians. (Tr. 146) The prime contractor dealt with computers and communications. (Tr. 148)

Applicant initially worked in computer-desktop support before being promoted to junior systems administrator. (Tr. 75) He was promoted after other employees were terminated due to inappropriate actions. (Tr. 75) He was promoted to the NOC as a novice

learning the job. (Tr. 76) His duties were to create and delete email accounts, to monitor the email server, to conduct morning security checks, and to operate the mail server. (Tr. 77, Tr. 94, SOR Answer) Daily and weekly scans were conducted of all computers, and every computer was required to have HBSS (host-based security system) and HIPS (host-based intrusion prevention system) software on them. (Tr. 94) Applicant had no knowledge about HIPS and no motivation to learn about HIPS. (Tr. 81) The HBSS was the software responsible for implementation of anti-intrusion tools and auditing. (SOR Answer)

HBSS and HIPS, which are designed for security over host-based systems dealing with intrusion and infections are dealt with at the individual workstation level, are particular to U.S. Government networks. (Tr. 67) HBSS and HIPS prevent plugging in a hard drive through a USB port. (Tr. 31) If HBSS was not installed on a workstation the systems administrators had to answer to the information assurance (IA) administrator. (Tr. 94)

In 2014, a civilian contractor at Applicant's worksite was arrested and subsequently convicted of espionage, child pornography, and child-sex crimes, among other crimes. (Tr. 53, 132) Around the same time, another civilian contractor was also fired and arrested for criminal activity. (Tr. 16, 42) When these individuals were removed, Applicant was given a promotion to work in the NOC. (Tr. 96)

As part of the FBI's investigation into the criminal conduct of the arrested contractors, the government witness, a cyber-security advisor (investigator), conducted an onsite network security evaluation and checked the IT system for additional problems. (Tr. 69), His findings are listed in Ex. 7. (Tr. 41) He looked for "back doors," and removed any pornography that was still on the network. (Tr. 17, 41) He reviewed and pulled information from over 600 machines on the Non-Secure Internet Protocol Router (NIPR) network. (Tr. 18) He was onsite for a week or more doing his inspection. (Tr. 70)

The investigator's findings from the June 2014 investigation were set forth in a September 9, 2014 email. (Ex.7) It was asserted that Applicant and a co-worker, both systems administrators, had disabled anti-intrusion tools on their workstations and information servers on the network they operated; there was improper placement of their workstations into elevated category groups within the directory, which would allow the two administrators to communicate unimpeded between workstations and servers while using the same network account, which violated Defense Information Security Agency (DISA) Security Technical Implementation Guides (STIGs); and Applicant's NIPR workstation had accessed websites, which contained content that included hate groups and other sites in violation of the IT system's use policy.

The investigator testified that his job was simply to collect the information, identify the issues, and present them. (Tr. 65) He explained that if the anti-virus or HBSS were off, there would be a logo on the monitor with a red "X" showing the items were disabled. (Tr. 66) The investigator discovered that Applicant's domain administrator account was also added to the local administrator's group, which would allow Applicant to make changes directly to his local machine as well as to servers and computers on the domain

as well. (Tr. 26) The investigator stated Applicant's account was never in the work station, but was in the server and should not have been there. (Tr. 167) The investigator stated, "I can't tell or see if he did it, however, it was in there and he had the accesses that would have allowed for that." (Tr. 167-168)

During the course his investigation, the investigator provided daily updates to the command. (Tr. 70) An out-briefing was given to the command listing all critical issues before the investigator left the installation. (Tr. 67) Any major issues or major findings were provided in an executive summary. (Tr. 68) About 80 percent of the information is given on site. (Tr. 60) The information is provided to criminal investigators to determine if anything illegal had occurred. (Tr. 68) After the information is collected it is reviewed and referenced against known bad lists, reviewed for malware and nation-state activity, and he then writes up a large report that goes into much more detail, which can sometimes take two months. (Tr. 50, 60) The investigator prepared a report that was based on events that occurred before the June 2014 inspection of the IT system that led to the discovery of Applicant's workstation in the elevated category group within the directory. A copy of the investigator's went to the criminal investigator and the director of security at the worksite. (Tr. 71) The report was based on events prior to the June 2014 inspection. The Applicant's removal from the installation occurred three months after the investigation was completed, in September 2014. (Tr. 63)

In September 2014, three months after the investigator completed his investigation, Applicant and a co-worker were told they had been reported for "suspicious activity." Applicant was removed from the installation, although he asserts he was never given any specifics as to the basis of the allegations or what the "suspicious activity" involved. Applicant and his employer made numerous requests to obtain information on the alleged incidents. (Ex. 9) Six months after he left the country, he and his employer still had not been told the nature of the alleged misconduct. (Tr. 79) He learned some details through a Freedom of Information Act request. (Tr. 80)

Regarding allegations that Applicant had disabled the anti-intrusion tools (Tr. 30), the event logs show the HBSS and HIPS were disabled multiple times. (Tr. 32) The IA government administrator was the only person who had the ability to disable the HBSS. (Tr. 168) The investigator stated having an account at the local administrator level would allow Applicant to access HBSS and disable the anti-intrusion tools. (Tr. 169)

A cyber-security advisor (investigator) testified for the government at Applicant's hearing. He asserted, and Applicant disagreed, that a local administrator such as the Applicant, had the ability to turn off and manipulate programs on specific machines. (Tr. 55) The AI administrator would call and say he wanted to turn the programs back on and Applicant told him "no." Applicant's employer disagrees with this statement, stating the AI administrator was responsible and had the authority to correct any violation of the Defense Information Systems Agency (DISA) standards. (Tr. 139) The investigator testified that the administrators started disabling the security programs themselves. (Tr. 55) There were daily and weekly scans performed by the AI administrator to make sure HBSS was on all machines except for two administrator machines and one or two servers,

which included Applicant's machine. (Tr. 48) When asked by Applicant about logs showing he had been the person to disable the HBSS and HIPS, the investigator stated "So it's going to be tough for me to really identify but you had the access and ability." (Tr. 63)

Applicant had a personal account and three separated administrative accounts which maintained 12 servers. His computer was on the NIPR network. As part of his duties, he would occasionally have to access a Secret Internet Protocol Router (SIPR) computer to create and delete accounts. He never had a computer or workstation on the SIPR network. (Tr. 90, SOR Answer) There was a centralized SIPR computer that was accessed by all systems administrators. (Tr. 90) Applicant testified that the HBSS and security breaches were said to be on the SIPR network. (Tr. 90)

Applicant's supervisor at the time of Applicant's alleged violations, the technical lead and desktop supervisor and manager, said he does not believe Applicant had the knowledge or experience to disable HBSS or to place his machine in a higher category of access. He said he was "an outstanding desktop tech but you [Applicant] was a junior sys admin, at best, so from my assessment, I don't think that you had the skill set to pull that part off." (Tr. 156) "That" being the violations asserted such as disabling HBSS and placing his machine in a higher category of access. He testified Applicant was always reliable and a stellar desktop technician, but when he moved to the NOC, he was new and green, and it would take time for him to learn his job. He stated, "So the things he was being accused to do, it just didn't make sense with his skill set." (Tr. 160) He said it would not have given any value added for Applicant to take the initiative to try to circumvent security protocols or do something on a high-end server. (Tr. 163) Any problems with information assurance and HBSS would have been handled by Applicant's management and not by Applicant. (Tr. 162)

Applicant asserts he never placed his account on any elevated or restricted group. (Tr. 78) He denied he had ever scanned his machine to determine the extent of his access rights. (Tr. 187) Whenever he had to perform a task requiring elevated rights, he had to have the assistance of more senior personnel. If he was helping a user who needed to get on an approved website, a website that had initially been flagged, he would have to contact the information assurance (IA) administrator to have the HBSS disabled. (Tr. 77, 121) The IA had a specific duty as the HBSS administrator to maintain the HBSS. (Tr. 139) Applicant acknowledged he believed there were personal problems between him and the IA administrator. (Tr. 83) The IA worked for the primary contractor and not Applicant's employer. (Tr. 149) Following the inspection, the IA administrator was terminated from his position before Applicant was removed from the installation. (Tr. 78)

Applicant had been told he would be trained in how to operate the Domain Name System (DNS) by a senior systems administrator. However, he was never trained in the system and he never logged onto the system. (Tr. 80) He does not know if, by being selected to be trained to operate the DNS server, he had been elevated for inclusion in an elevated category. Someone with authorization had moved him to the restricted

organizational unit (OU). He had no idea that he was in an elevated category or who placed him in an elevated category. (Tr. 122)

Applicant denies ever having the necessary access to make any changes to configure or disable anti-intrusion tools. (Ex. 10) Those tools were administered by the IA department. He stated he had no knowledge of how to configure or manipulate intrusion tools. Nor did he have the knowledge to disable security settings without assistance. (Ex. 10) Prior to the annual DISA inspection in July 2014, the same account served as his administrator's and user's account. (Ex. 10) After being told that to comply with new security measures, multiple accounts were needed. At that time, old accounts were disabled, and he was issued three administrator accounts. The reason for the security measure was to prohibit unimpeded communication between workstations and computers. He was not instrumental and did not take part in the creation of the new accounts. Nor was he involved in the placement of these accounts in any specific-security category group. (Ex. 10) The accounts were created by the AI office. If the accounts or workstations were placed in the wrong security category, it was done without his knowledge, as he had nothing to do with the creation or placement of these accounts. (Ex. 10) The only personnel who could place a workstation in an elevated status was an administrator account possessed by the NOC supervisor or AI personnel.

The president of the company onsite in 2014 stated in an April 9, 2015 email that the HBSS software had incorrect settings and had improper setup policies that prevented requested and required software from being installed. Due to the HBSS, incorrect settings and policies, all software that had utilized the directory would fail immediately, which included patches, flash patches, and Windows security updates, all of which were required to be installed. Disabling and re-enabling the software occurred regularly. The desktop support and systems administrators were prevented by the incorrect settings and policies from making the network safer by installing required security updates to the network. If the software was not temporarily disabled by the AI administrator, many of the computers on the network would not have been properly patched. (Ex. 9) Applicant always requested assistance from the AI administrator whenever he had to have the HBSS turned off.

The company's president also said there were no cyber-incident reports filed, which would have included log files, dates of proven incidents, login records, and additional information that would show illegal software or illegitimate reasons for disabling software in order to install required software and then re-enable the software. (Ex. 9) The HBSS failed the July 2014 DISA inspection due to improperly implemented policies and lack of training and policy templates that could have easily prevented the need to disable the software in order to install all other forms of software, patches, and security updates. (Ex. 9)

After his removal from the jobsite, Applicant stayed at the overseas location from September until November 2014, hoping to get the matter resolved and return to work. (Ex. 5) He eventually found out that his clearance had been flagged for misuse of unauthorized access and compromising government security. (Ex. 5) He contacted the

Inspector General (IG) for the Defense Security Services (DSS) and was told his clearance was pending, and he should wait for resolution of the investigation. In May 2016, Applicant contacted his congressman in an attempt to resolve the issue. The investigation was adjudicated in April 2017. (Ex. 5) Although his clearance is suspended, the original contractor he worked for at JTBF is still sponsoring his clearance application. (Ex. 5)

Regarding the hate-group content that was on his machine in 2014, Applicant explained that, from December 2007 to August 2011, he worked as a contractor for a federal law enforcement agency. In 2008 or 2009, while he was on temporary duty (TDY) in Washington DC, he met a coworker who was working for the same agency. The coworker needed work done on his computer. (Tr. 91, Tr. 114) Applicant helped him with his computer problem and told the individual he could contact him if he had additional computer problems. Applicant did not associate with the individual and they were not friends. (Tr. 126) In January 2014, while overseas, Applicant learned the individual had founded a web site that was considered a hate site. The individual was later charged with operating a hate group. (Ex. 5) When Applicant learned the individual had been arrested he went to various sites to learn about the individual and about the arrest. (Tr. 113) He made the searches to learn about the individual. (Tr. 127) Applicant stated he had never accessed any hate group or had knowingly associated with any hate group members.

It was alleged Applicant's computer also had a large cache of hundreds of pictures of women that were cataloged and detailed by type and other attributes, which was not criminally illegal in nature, but did violate NIPR use policy. (Ex. 7, Ex. 8) Applicant denies the allegations. (Ex. 10) He asserts he never accessed a website with content that violated the acceptable use policy. (SOR Answer) He never received either a verbal or written notification by his supervisor of inappropriately accessing websites. He had photos on his computer, but the pictures were not unacceptable nor a violation of what is publically deemed acceptable violating the acceptable use policy. (SOR Answer) He also denies there were hundreds of pictures.

The investigator testified most of the pictures of women appeared to come from Facebook and none were pornographic. (Tr. 37) Applicant stated all photographs came from Facebook and did not violate the terms of his computer use. (Tr. 89) There were over 100 photos of women on Applicant's workstation, which was not illegal, but the investigator asserts were against policy. (Tr. 38) The investigator had reviewed a few of the photos. (Tr. 58) He said "I only looked into a few to see enough that I needed to see." (Tr. 166) The investigator did not review all of the files. (Tr. 65) One photo he viewed reportedly was of a topless woman bending over a motorcycle. (Tr. 58) There were no zone identifiers of those files, and the investigator stated they "probably could" have come from Facebook. (Tr. 59) The photos were not shown to be pornographic. (Tr. 39) These photos were under the Applicant's user profile. (Tr. 39) It was alleged the photos were organized into different folders. (Tr. 56) Applicant states there were no more than three folders, asserts all photos came from Facebook, and none contained nudity. (Tr. 125) He says Facebook had filters that prevent such nude photographs. (Tr. 116) He vehemently denied any intention to view pornographic images. (Tr. 82)

Applicant asserts all the pictures came from Facebook and public profiles and were not pornographic. (Tr. 81) He stated,

> I vehemently dispute the willingness to look at anything pornographic, anything illegal or anything of that nature that I felt would violate the terms of use. Those were public profile pictures, and none of which were pornographic. (Tr. 82)

In Applicant's September 2017 enhanced subject interview, he stated he discovered through a FOIA response that he was suspected of disabling intrusion tools, which granted his workstation improper placement on elevated category groups. During the interview, he stated he had no knowledge of how to configure his machine, did not have rights to alter his software, and did not have access to carry out the task. (Ex. 5) He said he did not know what happened, and was not involved in any way. In his June 2016 and September 2017 interviews, he indicated his clearance had been suspended. The suspension was discussed in his June 2016 interview. (Ex. 5)

Applicant's employer was given very little information about what happened and never had a chance to actually look at the evidence, make a response to it, or provide an explanation. (Tr. 132) Although as a junior employee Applicant had the least responsibility, he was listed as backup on organizational charts because every position required a second systems administrator to be listed for every server or function. (Tr. 137) His employer attests Applicant was still learning did not have the skill set and knowledge to perform many systems administrator tasks. (Tr. 137)

Character Information

The president of the company for which Applicant worked as a contractor in 2014 stated Applicant "was professional, competent, honest, and showed no signs of being a security risk. From what we have been able to learn thus far about the alleged security incident, it is our opinion that he is not guilty of the accusations. . ." (SOR Answer) He testified the actions listed in the incident summary would have been out of character for Applicant and impossible for Applicant to execute based on the level of access Applicant had in his position as junior systems administrator. The incident report disregards that certain network security tools were disabled by senior systems administrators with full knowledge of the U.S. military, local IA staff, and DISA inspectors due to technical problems with the government network. (SOR Answer)

Applicant's manager and direct supervisor from 2015 through 2017 are of the opinion Applicant was a truly valuable asset. He showed himself to be honest, dependable, and incredibly hard-working. He was an impressive problem solver who was always able to address complex and challenging issues with confidence. (SOR Answer) He has never improperly handled any company equipment or sensitive information. He was not written up or disciplined for any behavior. The manager stated Applicant was a

true team player, a joy to work with, and a dedicated and knowledgeable employee. (SOR Answer)

Applicant's supervisor overseas during his work for the U.S. military stated Applicant was always extremely detail-oriented and never mishandled classified information, sensitive data, or customer's Personally Identifiable Information (PII). He never received a single customer complaint about Applicant. (Ex. A) Applicant was a trusted and well-valued member of the team. Given the opportunity, he would hire Applicant without reservation as well as recommend him for other IT positions, either civilian, contractor, or federal. (Ex. A)

Policies

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 must 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 overarching adjudicative goal is a fair, impartial, and commonsense decision. According to AG ¶ 2(a), the adjudication process is an examination of a sufficient period and a careful weight of a number of variables of an individual's life to make an affirmative determination that the individual is an acceptable security risk. This is known as the whole-person concept.

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 the applicant may deliberately or inadvertently fail to safeguard classified information.

Such decisions entail a certain degree of legally permissible extrapolation of potential, rather than actual, risk of compromise of classified information.

Section 7 of Executive Order 10865 provides that decisions shall be "in terms of the national interest and shall in no sense be a determination of 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

Use of Information Technology

AG ¶ 39 articulates the security concern for use of information technology:

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

AG ¶ 40 describes conditions that could raise a security concern and may be disqualifying including:

> (a) unauthorized entry into any information technology system;
>
> (b) unauthorized modification, destruction, or manipulation of, or denial of access to, an information technology system or any data in such a system;
>
> (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;
>
> (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;

(g) negligence or lax security practices in handling information technology that persists despite counseling by management; and

(h) any misuse of information technology, whether deliberate or negligent, that results in damage to the national security.

SOR ¶ 1.a alleges Applicant was terminated in August 2011 for plugging an unauthorized hard drive into a government computer in 2011, without authorization. This was a violation of IT policies and procedures. SOR ¶ 1.b asserts Applicant violated his administrative privileges on the SIPR and NIPR networks. It is alleged Applicant permanently disabled anti-intrusion tools on his workstation, improperly placed his workstation into elevated category groups within the directory, and modified his system configuration to violate and obfuscate security requirements and auditing. SOR ¶ 1.c alleges Applicant repeatedly accessed websites with content in violation of the Acceptable Use Policy and improperly loaded pictures of women on his workstation. SOR ¶ 1.d alleges Applicant's access to classified information was suspended on March 27, 2015.

Regarding the conduct alleged in SOR ¶¶ 1.b and 1.c, the government investigator testified that Applicant had been placed in an elevated category group, but that he did not know who had placed Applicant in the group. He could not say if it had been done by Applicant. There were no Cyber Incident reports filed, which would have included log files, dates of proven incidents, login records, and additional information showing illegal software or illegitimate reasons for disabling software in order to install required software and then re-enable the software. Applicant asserts he never placed his account on any restricted group and never scanned his machine to determine what access he had.

Whenever he had to perform a task requiring elevated rights, he obtained the assistance of more senior personnel. He would contact the IA administrator when the HBSS had to be disabled. The IA administrator's duty was to maintain the HBSS.

A senior systems administrator had told Applicant he would be trained in how to operate the DNS. However, Applicant was never trained in the system and never logged onto the system. He posited that maybe his selection to be trained had resulted in him being placed in other categories. Someone with authorization had elevated him to the restricted organizational unit. He has no idea that he was in an elevated category or who placed him in that category.

Applicant always requested assistance from the AI administrator whenever he had to have the HBSS turned off. He asserted he did not have the knowledge, administrative rights, or the technical skills necessary to modify system configurations to disable the HBSS. Applicant's supervisor at the time, the technical lead and desktop supervisor and manager, said Applicant was an outstanding desktop technician, but was a junior systems administrator and did not have the skill to make the changes Applicant was accused of in the SOR. He indicated Applicant was always reliable and a stellar desktop technician, but when promoted to the NOC, he was new and green and it would take time for him to learn

his job. He said disabling the HBSS would not have given any value added for Applicant to take the initiative to try to circumvent security protocols or do something on a high-end server.

Applicant's employer testified the conduct alleged in the SOR would have been out of character for Applicant and impossible for Applicant to execute based on the level of access Applicant had in his position as junior systems administrator. Additionally, he testified the incident report by the government investigator disregards that certain network security tools were disabled by senior systems administrators with full knowledge of the U.S. military, local IA staff, and DISA inspectors due to technical problems with the government network.

Applicant vehemently disputes any intention or willingness to view anything pornographic, anything illegal, or anything of the nature that would violate the terms of the Acceptable Use Policy. He asserts the photos found on his workstation were public profile pictures, and none of which were pornographic. The government investigator conceded that he had only looked at a few of the pictures and conceded the pictures could have come from Facebook and were not illegal to have on Applicant's computer. This was not a violation of the Acceptable Use Policy.

While working for a previous employer in Washington D.C., Applicant met a coworker working for the same agency who had computer problems. Applicant helped him with his computer problems. They were not friends. When Applicant later learned the individual had been arrested for operating a hate site, he went to various sites to learn about what the individual was doing. His searches for information were not a violation of the Acceptable Use Policy.

I find the statements of Applicant, his former supervisor, and former employer to be credible. Applicant had access at an elevated level, but there is no evidence he put himself in the elevated group. Anti-intrusion tools were turned off, but Applicant had no ability to do so, and former supervisor said there was no advantage for Applicant to do so. The allegations (SOR ¶ 1.b and SOR ¶ 1.c) made under the use of information technology guideline are not substantiated. Even if the allegations were not unsubstantiated, they would be mitigated under AG ¶ 41(a), *infra*. The alleged conduct was not recent.

AG ¶ 41 describes conditions that could mitigate security concerns include:

> (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.

SOR ¶ 1.a asserts Applicant was terminated from his employment eight years ago. Applicant admits he plugged the hard drive into his government computer resulting in his termination. He freely admitted his error and discussed the events and termination in both his OPM interviews. He listed it on his January 2012 e-QIP, his January 2012 Declaration of Federal Employment, and his July 2017 e-QIP. He told his prospective employer about it when he applied for the overseas position. His employer contacted the other company and was told the incident occurred as Applicant had explained it. He said it was a lapse of judgment, that it was a mistake, and was an isolated incident. Applicant testified that it was not malicious in nature and under no circumstance was it meant to be a security breach or anything that would endanger the government system. It was a simple lack of judgment which cost him employment.

Applicant acknowledges his actions involving the hard drive were shortsighted and thoughtless and that there was no excuse or justification for his unethical act. The action was not characteristic of how he handled business before or after the incident. This was his first offense at the company, and he testified he was not running away from it. When confronted, he acknowledged his mistake and did not make or offer an excuse for the incident.

The action is mitigated under AG ¶ 41 (a). So much time has elapsed since the behavior happened that it is unlikely to recur and does not cast doubt on Applicant's current reliability, trustworthiness, or good judgment.

Personal Conduct

AG ¶ 15 explains why personal conduct is a security concern stating:

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

Based on Applicant's response on his May 4, 2015 e-QIP to the employment inquiries regarding the reason why his employment ended in August 2011, following disqualifying condition potentially applies:

AG ¶ 16 (a): deliberate omission, concealment, or falsification of relevant facts from any personnel security questionnaire, personal history statement, or similar form used to conduct investigations, determine employment qualifications, award benefits or status, determine national security eligibility or trustworthiness, or award fiduciary responsibilities.

The personal conduct security concerns raised in the SOR may be mitigated by any of the following potentially applicable factors in AG ¶ 17:

(a) the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts;

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

(c) the offense is so minor, or so much time has passed, or the behavior is so infrequent, or it happened under such unique circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment;

(d) the individual has acknowledged the behavior and obtained counseling to change the behavior or taken other positive steps to alleviate the stressors, circumstances, or factors that contributed to untrustworthy, unreliable, or other inappropriate behavior, and such behavior is unlikely to recur;

(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.

SOR ¶ 2.a cross-alleges under the personal conduct guideline the same conduct alleged under the use of information technology guideline. The misuse of a government computer is explicitly covered under Guideline M. As previously discussed under the use of information technology guideline, Applicant did not violate his administrative privileges, did not modify his system configuration, did not place his workstation in an elevated category group, and did not use his workstation to violate the Acceptable Use Policy. He refuted the security concerns in that regard. The mitigating factors in ¶ 17.f. applies to the allegations in ¶ 1. b and ¶ 1.c. The conduct in allegation in ¶ 1.a occurred more than eight and a half years ago and has not been repeated. He exhibited reform by admitting his

mistake and fully acknowledging his actions. I conclude that conduct is unlikely to recur. It is mitigated under ¶ 17.d.

On Applicant's May 2015 e-QIP, he indicated he left his job in August 2011 due to end of contract and being released from the contract under mutual agreement. This is one question on one e-QIP that occurred more than four-and-a-half years ago. SOR ¶ 17.c applies to due to the passage of time and the behavior being infrequent. He did not fully describe he was terminated for plugging a hard drive into his government computer. However, he explained the termination for plugging in the hard drive on his January 2012 e-QIP and on his January 2012 Declaration for Federal Employment, and told his prospective employer at the JTFB about it, all of which occurred before he completed the May 2015 e-QIP.

Following Applicant's May 2015 e-QIP, he explained his 2011 termination in a September 2017 sworn statement. On his July 2017 e-QIP he fully explained in detail that he had connected a non-government external hard drive to test it on his government computer resulting in the termination of his employment. It was not established that Applicant deliberately falsified his July 2017 e-QIP by failing to disclose the details of his 2017 termination.

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), "[t]he ultimate determination" of whether to grant a security clearance "must be an overall commonsense judgment based upon careful consideration of the guidelines" and the whole-person concept. My comments under Guidelines M, use of information technology, and E, personal conduct, 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 general sense of the statements of a coworker, his employer, and two former supervisors is that Applicant is careful about safeguarding classified information, diligent, professional, responsible, trustworthy, reliable, and honest. Their statements support

reinstatement of his security clearance. The government investigator stated Applicant's workstation was in an elevated category, but he could not say who had put Applicant in that elevated category. Applicant vehemently denies he modified his system configuration to violate security requirements. He asserts he did not have the knowledge, administrative rights, or the technical skills necessary to modify system configurations to disable the HBSS. The HBSS was controlled by the AI administrator who was the only person who could disable the HBSS.

Applicant's supervisor does not believe Applicant had the ability to make the changes. The changes to circumvent security protocols or do something on a high-end server would not have given any value added for Applicant. There was no Cyber Incident report filed, which would have included log files, dates of proven incidents, login records, and additional information showing illegal software or an illegitimate reason for disabling software in order to install required software, and then re-enable the software. Applicant asserts he did not make the changes, and there is no evidence he did so.

Applicant viewed hate websites when an individual he knew made national news for running a hate site. He viewed these sites out of personal curiosity to learn of the accusations. He had photographs of women on his computer. The government investigator only viewed a few of the photographs and admitted the photographs could have come from Facebook as asserted by Applicant. Neither of these events violated the Acceptable Use Policy.

The law, as set forth in *Egan,* Exec. Or. 10865, the Directive, and the AGs, have been carefully applied to the facts and circumstances in the context of the whole person. The allegations in SOR ¶¶ 1.b, 1.c, and 2.a with respect to the alleged violations of administrative and access privileges, and 2.c are unsubstantiated. He mitigated the security concerns listed in ¶¶ 1.a, 1.d, 2.a with respect to the insertion of the hard drive, and 2.b. The record evidence leaves me without questions or doubts about his eligibility and suitability for a security clearance. For all these reasons, I conclude Applicant has mitigated the use of information technology and personal conduct security concerns.

Formal Findings

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

Paragraph 1, Guideline M:	FOR APPLICANT
Subparagraph 1.a – 1.d:	For Applicant
Paragraph 2, Guideline E:	FOR APPLICANT
Subparagraphs 2.a – 2.c:	For Applicant

Conclusion

In light of all of the circumstances presented by the record in this case, it is clearly consistent with the national interest to grant Applicant's eligibility for a security clearance. Eligibility for access to classified information is granted.

_____
Claude Heiny
Administrative Judge

,