DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
----------	)	ISCR Case No. 08-11762
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Daniel F. Crowley, Esquire, Department Counsel
For Applicant: *Pro se*

February 7, 2011

Decision

HARVEY, Mark, Administrative Judge:

Applicant violated security protocols. Although his violation of security rules was designed to facilitate mission accomplishment, his violations of information technology system security protocols are not mitigated at this time. Eligibility for access to classified information is denied.

Statement of the Case

On July 23, 2007, Applicant submitted an Electronic Questionnaires for Investigations Processing (e-QIP) version of a security clearance application (SF 86) (GE 1). On July 19, 2010, the Defense Office of Hearings and Appeals (DOHA) issued an SOR to Applicant, pursuant to Executive Order 10865, *Safeguarding Classified Information Within Industry,* dated February 20, 1960, as amended; Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (Directive), dated January 2, 1992, as amended; and the adjudicative guidelines (AG) promulgated by the President on December 29, 2005.

The SOR alleged security concerns under Guideline M (use of information technology systems). (Hearing Exhibit (HE) 2) The SOR detailed reasons why DOHA could not make the preliminary affirmative finding under the Directive that it is clearly consistent with the national interest to grant or continue a security clearance for Applicant and recommended referral to an administrative judge to determine whether Applicant's clearance should be granted, continued, denied, or revoked. (HE 2)

On August 9, 2010, the Defense Office of Hearings and Appeals (DOHA) received Applicant's response to the SOR allegations. (HE 3) Applicant requested a hearing. (HE 3) On November 1, 2010, Department Counsel indicated he was ready to proceed on Applicant's case. On November 8, 2010, DOHA assigned Applicant's case to me. On November 18, 2010, DOHA issued a hearing notice. (HE 1) Applicant waived his right to 15 days notice of his hearing. (Tr. 13-14) On November 22, 2010, Applicant's hearing was held. At the hearing, Department Counsel offered five exhibits (GE 1-5) (Tr. 20). There were no objections, and I admitted GE 1-5. (Tr. 21) Additionally, I admitted the hearing notice, SOR, and Applicant's response to the SOR as hearing exhibits. (HE 1-3) On December 1, 2010, I received the transcript. I held the record open until January 28, 2011, to permit Applicant to submit documentation. (Tr. 64-66, 108) On January 28, 2011, I received four additional documents from Applicant. (AE A-D) Department Counsel noted that a letter from Mr. B was hearsay and urged that it receive less weight. (AE A) Applicant's proffered exhibits are admitted.

Findings of Fact[1]

In Applicant's response to the SOR, he denied all of the SOR allegations. (HE 3) However, with respect to SOR ¶ 1.f, he said he received some training. (HE 3) His admissions are accepted as findings of fact.

Applicant is a 51-year-old employee of a defense contractor. (Tr. 5)[2] He received a master of science degree in electrical engineering in February 1982. (Tr. 5-6) He married in 1980 and divorced in 1985. His children were born in 1980 and 1981. His second marriage was in 1989, and he was divorced in 1998. Applicant has never served in the military. He did not disclose any illegal drug use or alcohol-related offenses on his July 23, 2007, SF 86.

Use of information technology systems

Applicant is a network professional with almost 30 years of experience. (Tr. 17, 48) Each of the incidents alleged in the SOR occurred. (Tr. 17) Applicant began working as a senior systems integration analyst for a major government contractor in April 2005. (GE 1) Applicant was responsible for installation, configuration, and

[1]Some details have not been included in order to protect Applicant's right to privacy. Specific information is available in the cited exhibits.

[2]Unless stated otherwise, the source for the information in this paragraph is Applicant's July 23, 2007 SF 86 and his resume. (GE 1, 5)

maintenance of a multi-million dollar network monitoring system (NMS). (GE 4) Applicant periodically downloaded software from his employer's site. (Tr. 43-44; GE 4) He said his downloads of patches were authorized by his manager. (GE 4) Applicant's manager, Mr. B, provided the following statement after the hearing:

> [Applicant's] job responsibilities included managing the [NMS]. This system required periodic maintenance that required downloading and installing software patches from the [NMS] company site. It also required other maintenance including, but not limited to providing "view only" controlled access to their [NMS] appliances via Webex, as well as other needed [NMS], as well as other needed [NMS] related activities. [Company] security was asked several times for the permission to conduct most of these activities and, in every case, permission (sometimes just verbal) was granted. (AE A)

The NMS downloads triggered intrusion detection systems. (GE 4) Applicant explained that security protocols often permit actions to occur which are forbidden even though the security protocols could stop the actions from occurring. It is like prohibiting entry through a door and then keeping "'the door open but we will shoot everybody who goes through that door.' That's the policy for lack of a better explanation." (Tr. 50)

On February 10, 2006, Applicant's employer issued a report of investigation (ROI) which cited him for several violations of information security rules. (GE 2) Applicant's SOR listed six allegations, which are all discussed in the ROI and at his hearing.

Applicant was working for about two weeks at the government worksite when he removed a laptop computer from a secure network, and allegedly connected the laptop computer to another government agency's network, and then connected the laptop computer back into the secure network. (Tr. 51-52; GE 2 at 1-2; SOR ¶ 1.a) Applicant said the laptop was not actually connected to other government agency's network. (Tr. 109) He used a data capture from the other government agency, and then used the laptop to evaluate the data capture. (Tr. 109)[3] The contractor purchased the laptop computer with special software valued at about $150,000 for use on a government computer network. (Tr. 28, 51) The laptop computer was not equipped with antivirus software or fully patched with updates. (GE 2 at 1-2; HE 2) Applicant was unaware that the laptop did not have adequate anti-virus software. (Tr. 39-40) Moving this laptop computer from a trusted network to an untrusted network, and then back to the trusted network, can compromise the trusted network because vulnerabilities are possibly transferred to the DoD's trusted network. (Tr. 28-29; GE 2 at 1-2; HE 2) A vulnerable computer or network is easier for a hacker to compromise. (Tr. 30) Applicant's supervisor asked him to use the laptop computer to troubleshoot the other network, and Applicant complied with the request. (Tr. 51-52) After he completed the mission, he was

[3] Evaluation of a "data capture" avoids the necessity for a connection to an untrusted network because the data is evaluated separately from the network.

complimented at a meeting for his successful endeavor. (Tr. 52) Because Applicant prudently used a "data capture" the DoD network was not compromised.

Applicant connected an encrypted tunnel to his home computer, which violated security controls and potentially created a tunnel to a private or commercial network. (GE 2 at 2; SOR ¶ 1.b) Theoretically, a tunnel to a home computer might have permitted a hacker or other person with malicious intent to use Applicant's home computer to bypass the DoD network's security systems. (Tr. 30-32) However, Applicant, as a computer expert, knew that his home network had superb anti-virus protection, and thus there was no danger posed to the DoD system by Applicant's violation of the rules. (Tr. 53) Applicant connected the DoD network to his home computer because he wanted to better accomplish the DoD mission, using some software resources on his home computer. (Tr. 52-53)

Applicant downloaded unauthorized streaming media software to his government computer. (Tr. 53-55; GE 2 at 2; SOR ¶ 1.c) Upon inspection, additional unauthorized software was found on his government computer. *Id*. Downloading non-approved software is a violation of Army regulations and creates a risk that a virus or other malicious logic will enter a government computer system through the software. (Tr. 32-33; GE 2 at 2; SOR ¶ 1.c) Applicant was responsible for a major application that was a new system, and he had to constantly download patches to about 20 servers to protect the integrity and functioning of the application. (Tr. 54-55) The first time he applied a patch from the website of the owners of the major application, the IDS detected the download and Applicant talked to security. (Tr. 55, 93) This was the only occasion he advised security of downloading a patch. (Tr. 93) Applicant told his manager that the only way to keep the system running was to download and install the patches and his manager told Applicant to go ahead and do it. (Tr. 55; AE A) He believed his manager talked to security a couple times about it, and his manager was not reprimanded later for absence of security's advance permission to download the patches. (Tr. 56; AE A) In addition, at the direction of another government contractor, Applicant connected the server to a bulletin board type system without pre-authorization from security. (Tr. 56, 72-73, 93; GE 2 at 2) The bulletin board was for customer service and allowed customers to efficiently report problems, and it allowed Applicant's company to document resolution of those problems. (Tr. 57) Applicant's goal was not to violate security. His goal was to improve efficiency and customer service. (Tr. 76) Applicant said everyone was aware of the bulletin board system's use. (Tr. 57)

On February 3, 2006, Applicant used a WebEx[4] through a secure DoD server to contact a vendor-contractor.[5] His use of the server circumvented security controls. (Tr. 45; GE 2 at 2; SOR ¶ 1.d) His objective was not to circumvent security. (Tr. 58-59) The

[4] A WebEx is an application sharing and conferencing service that allows those who are in conference together to see manipulations on their computer screens. In this case, those persons in conference could see information and applications on the DoD server.

[5] SOR ¶ 1.d (the transcript erroneously states SOR ¶ 1.e) was amended with the consent of the parties to conform with the allegation as stated in the February 10, 2006 ROI. (Tr. 96-97)

intrusion detection system would not detect the intrusion because the use of a WebEx appears to be normal traffic. (Tr. 83-84) His goal was to correct a technical problem with a server. (Tr. 59) Applicant used a WebEx conference with a third party without prior approval from security. (Tr. 34-37, 45-46; GE 2 at 1) The third party,[6] the vendor that licensed some very expensive software to DoD (software valued at several hundred thousand dollars), was located on the West Coast and the system with a problem was on the East Coast. Applicant did not want the delay and expense of having experts travel from the vendor's location to the East Coast to work on the server. Applicant permitted the vendor to have remote access to the DoD server over the Internet to check the server. (Tr. 58) Of the five security violations alleged in the SOR, the use of the WebEx conference device to probe a DoD secure server was the most serious because "an uncleared person" from a vendor-corporation "is coming in and looking inside a government computer" without the permission or knowledge of security personnel. (Tr. 83, 86) Applicant was able to observe the actions of the vendor, and he believed he would be able to prevent, and did prevent the vendor from abuse of the DoD server. (Tr. 58, 85) Applicant said his corporate supervisors authorized him to use the WebEx, and one supervisor actually participated in the WebEx with Applicant and the third-party vendor. (Tr. 90; AE A) Nevertheless, even if Applicant had explained his plan to conduct the WebEx and allow the vendor to troubleshoot the problem under his direct observation, security would have disapproved this proposal. (Tr. 86-87) Applicant disclosed the use of WebEx to security after the fact. (GE 2) However, this breach of security rules occurred after Applicant received information assurance awareness training. *Id*.

Applicant used a contractor-owned laptop and software that was purchased to work on a DoD contract for a contract with another federal government agency. (Tr. 40, 62; SOR ¶ 1.e) Applicant was the only source of this information. (Tr. 40) Applicant said his supervisors at the government contractor asked him to use the laptop and software to assist the other federal government agency. (Tr. 41-42, 63) Applicant said he was permitted to use the software on multiple contracts for multiple agencies, and a government witness said the use of the laptop and software was restricted to DoD contracts. (Tr. 80, 91) It is possible that the use of the software was restricted to a particular laptop, and not to a particular government agency. (Tr. 81) The licensing contract was not provided, and Applicant likely had more direct knowledge of licensing restrictions than other witnesses. (Tr. 91) I conclude the allegation that Applicant violated the license for the laptop and its software is not substantiated. Nevertheless, as stated in SOR ¶ 1.a, *supra*, if there was a connection of the laptop and software to another government agency network, the connection would risk the compromise of the DoD network, when it was connected back into the DoD network because vulnerabilities in the other government agency network could have been transferred to the DoD network. (Tr. 81-82) Applicant conceded that from a security standpoint "it was probably not a wise decision;" however, he was under direct orders to assist the other government agency. (Tr. 63)

[6] Applicant subsequently received employment from the vendor, and then his employer in 2005 purchased the vendor's company. (Tr. 59-60)

After each security-related information technology incident, Applicant received oral warnings and subsequently he received information-awareness training. (Tr. 66; SOR ¶ 1.f) He said he told security the first time he downloaded software, and the response was to go ahead. (Tr. 67) The security person providing approval would then contact the intrusion detection team and let them know that the intrusion or download was approved. (Tr. 78) Applicant was involved in various intrusions, which set off alarms, and resulted in investigations being initiated or opened. (Tr. 79)

There is flexibility in security and information assurance. The network has a designated approval authority (DAA) who is supposed to make decisions, where security processes and procedures can be violated or waived in order to accomplish the mission or improve efficiency. (Tr. 74, 77)

When Applicant left his employment with the contractor, he received an award. His departure was under positive terms. (Tr. 18, 59, 70; AE B)

Applicant contended that he knew exactly what he was doing at all times, and the DoD information technology system was never at risk. (Tr. 109) He insisted he would have shown poor judgment, if he had challenged the orders of his bosses. (Tr. 110)

Policies

The U.S. Supreme Court has recognized the substantial discretion of the Executive Branch in regulating access to information pertaining to national security emphasizing, "no one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988). As Commander in Chief, the President has the authority to control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to have access to such information." *Id*. at 527. The President has authorized the Secretary of Defense or his designee to grant applicant's eligibility for access to classified information "only upon a finding that it is clearly consistent with the national interest to do so." Exec. Or. 10865, *Safeguarding Classified Information within Industry* § 2 (Feb. 20, 1960), as amended and modified.

Eligibility for a security clearance is predicated upon the applicant meeting the criteria contained in the adjudicative guidelines. These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, these guidelines are applied in conjunction with an evaluation of the whole person. An administrative judge's overarching adjudicative goal is a fair, impartial, and commonsense decision. An administrative judge must consider all available, reliable information about the person, past and present, favorable and unfavorable.

The Government reposes a high degree of trust and confidence in persons with access to classified information. This relationship transcends normal duty hours and endures throughout off-duty hours. Decisions include, by necessity, consideration of the possible risk the applicant may deliberately or inadvertently fail to protect or 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. Clearance decisions must be "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." *See* Exec. Or. 10865 § 7. *See also* Executive Order 12968 (Aug. 2, 1995), § 3.1. Thus, nothing in this Decision should be construed to suggest that I have based this decision, in whole or in part, on any express or implied determination as to applicant's allegiance, loyalty, or patriotism. It is merely an indication the applicant has not met the strict guidelines the President and the Secretary of Defense have established for issuing a clearance.

Initially, the Government must establish, by substantial evidence, conditions in the personal or professional history of the applicant that may disqualify the applicant from being eligible for access to classified information. The Government has the burden of establishing controverted facts alleged in the SOR. *See Egan*, 484 U.S. at 531. "Substantial evidence" is "more than a scintilla but less than a preponderance." *See v. Washington Metro. Area Transit Auth.*, 36 F.3d 375, 380 (4th Cir. 1994). The guidelines presume a nexus or rational connection between proven conduct under any of the criteria listed therein and an applicant's security suitability. *See* ISCR Case No. 95-0611 at 2 (App. Bd. May 2, 1996).

Once the Government establishes a disqualifying condition by substantial evidence, the burden shifts to the applicant to rebut, explain, extenuate, or mitigate the facts. Directive ¶ E3.1.15. An applicant "has the ultimate burden of demonstrating that it is clearly consistent with the national interest to grant or continue his security clearance." ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002). The burden of disproving a mitigating condition never shifts to the Government. *See* ISCR Case No. 02-31154 at 5 (App. Bd. Sep. 22, 2005). "[S]ecurity clearance determinations should err, if they must, on the side of denials." *Egan*, 484 U.S. at 531; *see* AG ¶ 2(b).

Analysis

Upon consideration of all the facts in evidence, and after application of all appropriate legal precepts, factors, and conditions, I conclude the relevant security concerns are under Guideline M (use of information technology systems).

Use of Information Technology Systems

AG ¶ 39 articulates the security concern relating to use of information technology systems problems:

> Noncompliance 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 Systems include all related computer hardware, software, firmware, and data used for the communication, transmission, processing, manipulation, storage, or protection of information.

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

> (a) illegal or unauthorized entry into any information technology system or component thereof;
>
> (b) illegal or unauthorized modification, destruction, manipulation or denial of access to information, software, firmware, or hardware in an information technology 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 information on or to any unauthorized software, hardware, or information technology system;
>
> (e) unauthorized use of a government or other information technology system;
>
> (f) introduction, removal, or duplication of hardware, firmware, software, or media to or from any information technology system without authorization, when prohibited by rules, procedures, guidelines or regulations;
>
> (g) negligence or lax security habits in handling information technology that persist despite counseling by management; and
>
> (h) any misuse of information technology, whether deliberate or negligent, that results in damage to the national security.

AG ¶¶ 40(a) and 40(b) do not apply because Applicant did not engage in any "illegal or unauthorized entry into any information technology system or component thereof," or any "illegal or unauthorized modification, destruction, manipulation or denial of access to information, software, firmware, or hardware in an information technology system." AG ¶¶ 40(c) and 40(d) do not apply because he did not use "any information technology system to gain unauthorized access to another system or to a compartmented area within the same system," and he did not download, store, or transmit any "classified information on or to any unauthorized software, hardware, or information technology system." AG ¶ 40(h) does not apply because there is no evidence of any "damage to the national security."

AG ¶¶ 40(e), 40(f), and 40(g) apply because security personnel did not authorize Applicant's use of WebEx software through a secure DoD server to contact a vendor-contractor, and his use of WebEx is prohibited by "rules, procedures, guidelines or regulations." (SOR ¶ 1.d)[7] Applicant received counseling about security procedures in

[7] Applicant's use of WebEx, as alleged in SOR ¶ 1.d, is the only unmitigated security violation. He either refuted the other SOR allegations or demonstrated that he acted in good faith, being fully

handling information technology after he violated procedures. He subsequently used WebEx without permission, which was a breach of security protocols. Further inquiry about potential applicability of mitigating conditions is required.

Three conditions under 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 only in the interest of organizational efficiency and effectiveness, such as letting another person use one's password or computer when no other timely alternative was readily available; and
>
> (c) the conduct was unintentional or inadvertent and was followed by a prompt, good-faith effort to correct the situation and by notification of supervisor.

Applicant's conduct does not warrant full application of any mitigating conditions. On February 3, 2006, Applicant used a WebEx through a secure DoD server to contact a vendor-contractor. The vendor-contractor located on the West Coast, using WebEx entered a DoD server on the East Coast and moved about within the DoD server, attempting to troubleshoot a problem. Security or another authorized entity did not monitor the movement within the DoD server. The vendor-contractor did not receive any vetting or clearance from security. This was a significant breach of security that occurred after Applicant was counseled on several occasions about security requirements. Applicant is exceptionally knowledgeable about information technology. He has an outstanding understanding of the risks involved. Although there is no proof that Applicant's conduct caused any damage to national security, if other contractors were allowed on their own authority to clearly breach important security requirements, anarchy would result. Damage to national security would be inevitable because others who lack Applicant's experience and skill would not properly monitor the breach of security, or would take risks, assuming they had the requisite skill and knowledge to prevent damage to the information technology systems.

At Applicant's hearing, he emphasized his good-faith desire to accomplish his mission and his company's requirements; however, he acknowledged the vendor-contractor, who breached security protocols, could have traveled to the DoD server, as opposed to using the WebEx. Additionally, Applicant could have sought security approval or a waiver from the designated approval authority, and he did not do so. Because Applicant was unwilling to fully accept the DoD security requirements as

---

knowledgeable that his actions would not cause actual harm to security. His violations of security rules were based on the belief that they would facilitate mission accomplishment, and it is noteworthy that in 2005-2006, when the violations occurred, he had very limited experience working with DoD security.

trumping his or his company's perception of mission requirements, I am not convinced that the breach of security occurred under such circumstances that it is unlikely to recur. There is some residual doubt about whether Applicant is fully committed to complying with security requirements when those requirements result in inefficiency or compromise timely mission accomplishment. His presentation of mitigation evidence is insufficient to fully mitigate use of information technology systems security concerns.

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(a):

> (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.

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. AG ¶ 2(c). I have incorporated my comments under Guideline M in my whole-person analysis. Some of the factors in AG ¶ 2(a) were addressed under those guidelines, but some warrant additional comment.

Although the rationale for reinstating Applicant's clearance is insufficient to support a security clearance at this time, there are several factors tending to support approval of his clearance. Applicant is 51 years old, and he is sufficiently mature to understand and comply with security requirements. He received a master of science degree in electrical engineering. Applicant is a network professional with almost 30 years of experience. In 2005-2006, as a senior systems integration analyst for a major government contractor, Applicant was responsible for installation, configuration, and maintenance of a multi-million dollar network monitoring system. He worked diligently on this project, and his employer praised him for his hard work and superb results. His most recent security violation was in February 2006, which is not recent. He deserves substantial credit for volunteering to support the U.S. Government, as an employee of a contractor. There is every indication that he is loyal to the United States and his employer. There is no evidence that he abuses alcohol or uses illegal drugs. I give Applicant substantial credit for admitting most of the underlying facts relating to the breaches of security, as alleged in the SOR. These factors show some responsibility, rehabilitation, and mitigation.

The whole-person factors against reinstatement of Applicant's clearance are more substantial at this time. Applicant violated security rules relating to information technology. He was counseled about compliance with security rules. For example, security rules were violated when patches were installed without advance permission from security. Applicant observed that when permission to install patches was sought, it was always granted, and when patches were downloaded without security's permission, no adverse action beyond oral discussions with security personnel resulted. Applicant interpreted this as a green light to install patches without security permission. He was exceptionally knowledgeable about information technology issues, and he had a tendency to believe his expertise allowed him to violate security rules, which are primarily designed to protect information technology systems from software downloads and other information technology-related actions by those without his expertise. He was aware of the security requirement to seek permission before using software such as WebEx on a secure server. Nevertheless, he allowed a vendor-contractor to enter the DoD server through a secure DoD server using WebEx, which is a major violation of DoD security protocols. This breach of security was unnecessary because Applicant could have taken other actions to meet mission requirements. He should have sought permission from security or the designated approval authority for that system to undertake the WebEx, and explained the option of bringing an expert from the West Coast to the server location on the East Coast to make on-site repairs. Ultimately, it was not Applicant or his company's decision whether security protocols should be violated or waived for reasons of mission accomplishment. Moreover, Applicant's reliance on his project manager's statement is misplaced. His project manager does not have the authority to authorize Applicant to violate security rules and protocols. I am not convinced Applicant would comply with DoD security protocols or seek a waiver, if he viewed those DoD security protocols as frustrating his efforts to accomplish his company's mission.

I have carefully applied the law, as set forth in *Department of Navy v. Egan,* 484 U.S. 518 (1988), Exec. Or. 10865, the Directive, and the AGs, to the facts and circumstances in the context of the whole person. I conclude use of information technology systems security concerns are not fully mitigated, and he is not eligible for access to classified information at this time.

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 to 1.c:	For Applicant
Subparagraph 1.d:	Against Applicant
Subparagraph 1.e:	For Applicant
Subparagraph 1.f:	Against Applicant

Conclusion

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

_____
MARK HARVEY
Administrative Judge