DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 10-06328
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Phillip J. Katauskas, Esquire, Department Counsel
For Applicant: John F. Mardula, Esquire

January 13, 2012

Decision

CREAN, Thomas M., Administrative Judge:

Based on a review of the pleadings, exhibits, and testimony, eligibility for access to classified information is denied.

Statement of the Case

Applicant submitted an Electronic Questionnaire for Investigations Processing (e-QIP) on April 28, 2010, to obtain a security clearance required for employment with a defense contractor. After an investigation conducted by the Office of Personnel Management (OPM), the Defense Office of Hearings and Appeals (DOHA) issued an interrogatory to Applicant to clarify or augment potentially disqualifying information in his background. After reviewing the results of the background investigation and Applicant's response to the interrogatory, DOHA could not make the preliminary affirmative findings required to issue a security clearance. On March 17, 2011, DOHA issued Applicant a Statement of Reasons (SOR) detailing security concerns arising from his use of information technology systems (Guideline M), personal conduct (Guideline E), and financial considerations (Guideline F). The action was taken under Executive Order 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; Department of Defense Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and

the adjudicative guidelines (AG) effective in the Department of Defense on September 1, 2006. Applicant received the SOR on April 5, 2011.

The SOR alleges that Applicant was terminated by a previous employer for failure to comply with rules, procedure, guidelines, and regulations pertaining to information technology systems for use of Government furnished computers, adding unauthorized software to Government owned computer systems, accessing, viewing, and storing pornographic material on a Government furnished computer, and attempting to cover-up his improper use of the computer equipment. (SOR 1. a, and 2.a) Applicant answered the SOR on June 21, 2011. He admitted in part and denied in part the allegations with explanation. The SOR also sets forth 13 allegations of delinquent debts. (SOR 3.a to 3.m) Applicant denied these allegations in part. He admitted he had delinquent debts, but stated that the debts were paid or being paid. Applicant requested a hearing. Department Counsel was prepared to proceed on September 1, 2011, and the case was assigned to another administrative judge on September 9, 2011. DOHA issued a Notice of Hearing on September 16, 2011, scheduling a hearing for October 19, 2011. I was assigned the case on the day of the hearing and convened the hearing as scheduled. The Government offered four exhibits, which were marked and admitted into the record without objection as Government Exhibits (Gov. Ex.) 1 through 4. Applicant and one witness testified. Applicant offered 19 exhibits which I marked and admitted into the record without objection as Applicant Exhibits (App. Ex.) A through S. I kept the record open for Applicant to submit additional documents. Applicant timely submitted two additional documents which I marked and admitted into the record without objection as Applicant Exhibits T and U. Department Counsel had no objection to the admission of the additional documents. (Gov. Ex. 5, Memorandum, dated November 1, 2011) DOHA received the transcript of the hearing (Tr.) on October 25, 2011.

Findings of Fact

Applicant's admissions to portions of the SOR allegations are included in my findings of fact. After a thorough review of the pleadings, transcript, and exhibits, I make the following essential findings of fact.

Applicant is 38 years old and has worked as an information assurance security manager for a defense contractor since April 2010. He received a bachelor's degree in internet technology in 2005, and is studying for a master's degree in information technology. He served four years on active duty in the Marine Corps and four years in the Marine inactive reserves. He is married with four children. His monthly net pay is $7,156, with monthly expenses of $3,000, leaving $4,100 monthly in discretionary funds. His wife works part time. Applicant and his wife are current with their bills and taxes. (Tr. 41-45, 98-99, 109-111; Gov. Ex. 1, e-QIP, dated April 28, 2010; Gov. Ex. 4, e-QIP pages 6-10, dated March 2, 2007; App. Ex. R, Pay Stub, dated June 6, 2011)

After leaving active duty with the Marine Corps, Applicant was employed by a Government contractor working at a Government agency location from November 1999 until March 2000, when the contract was completed. From March 2000 until March

2009, he was employed by the same contractor working as a network administrator at a defense agency. He was terminated by the defense contractor for violation of its policy and the Government policy concerning computer use. He was unemployed from March 2009 until September 2009. During this time, he took a computer course to be certified as an information systems security professional. He was then employed as an information systems security officer by a private firm from September 2009 until April 2010. He commenced employment with his present defense contractor employer on April 2010 as a senior information systems security officer. (Tr. 40-43, 52-54; Gov. Ex. 1, e-QIP, dated April 28, 2010: *See also* Response to SOR, dated June 21, 2011, Attachments B through F)

The SOR alleges and a credit report establishes medical delinquent debts of $440 (SOR 3.a), $777 (SOR 3.b), $122 (SOR 3.c), $79 (SOR 3.d), $15 (SOR 3.e), $62 (SOR 3.f), $23 (SOR 3.g), $132 (SOR 3.h), $30 (SOR 3.i), and $30 (SOR 3.j); a credit account with a retail store charged off for $165 (SOR 3.k); a credit card debt charged off for $5,523 (SOR 3.l); and a mortgage foreclosure for $308,000 (SOR 3.m). (Gov. Ex. 3, Credit Report, dated January 5, 2011)

The medical debts were incurred for Applicant's and his family members' emergency medical treatment. Most of the bills were in his wife's name. The employers' medical plan at the time of treatment did not cover all their medical costs. Most of the bills were in his wife's name. He was unaware of the debt until he received the SOR. He has since paid the medical debts at SOR 3.a, 3.d, 3.e, 3.f, 3.g, 3.h, 3.i, and 3.j. (Tr. 63-72; App. Ex. F, Credit Statement, dated September 23, 2011; App. Ex. G, Bank Statement, dated June 9, 2011)

The medical debt at SOR 3.b for $777 is a remainder of a bill not completely covered by his present health insurance. Applicant makes monthly payments of $100 on this debt and the balance left at the time of the hearing was $377. He plans to pay the debt in full by the end of 2011. (Tr. 72-77, 79-80; App. Ex. H, Receipts, dated May 25, 3011; App. Ex. I, Receipts, dated October 15, 2011)

Applicant disputes the medical debt at SOR 3.c because he is unsure what medical treatment caused the debt. He checked with the medical treatment facilities and providers he and his family use and they are unable to confirm the debts. He intends to pay the debt when he learns of the origin of the debt. (Tr. 77-79, 106-109)

The $160 delinquent debt to the retail store at SOR 3.k has been paid in full. (Tr. 79-82; App. Ex. J, Bank Statement, dated March 15, 2011) The debt at SOR 3.l is for a credit card that Applicant used when he was unemployed. When he found employment, he negotiated a settlement of the debt for $2,500, and a payment plan. He paid $368 monthly and the debt has been paid in full. (Tr. 82-87; App. Ex. K, Bank Payments, various dates; App. Ex. L, Creditor Statements, various dates; App. Ex. U, Bank Statement, dated October 1, 2011)

On April 18, 2005, Applicant purchased a house for $300,000 at the height of the house market. When he lost his job in 2009, he could not make the mortgage payments.

The balance on his account was $238,000. By this time, the house value had declined drastically to approximately $145,000. He attempted to negotiate a loan modification plan but since he was unemployed he was unable to arrange a plan. Applicant tried a short sale but the creditor would not permit a short sale. The creditor foreclosed the house and purchased it for $110,000. The creditor subsequently resold the house. The creditor is not seeking a deficiency judgment against Applicant. (Tr. 87-96; App. Ex. M through R, Real Estate Documents, various dates)

While working for the Government contractor in 2006, Applicant received both a company laptop computer and a Government furnished computer from his company. He knew the second laptop was a Government supplied computer. He used both laptops to connect to the Government run network as required for his work with the company for the Government agency. In 2006, he installed software on the company and Government computers to assist him in doing his job. He did not have permission to install the software.

He initially testified that in 2008, he used the company computer to view adult pornography from the Internet. He said he did not use the Government computer to view or download pornography. In his response to the SOR, Applicant again stated he used the company laptop to view the pornography. At the hearing in response to questions from his counsel, Applicant testified that he had a personal internal computer network at his home. He used a router to connect his personal desktop computer, company laptop computer, and Government laptop computer. He viewed pornography on his personal desktop computer. The viruses from the pornographic site infected his company and government laptops, thereby infecting the Government network. In response to questions from Department Counsel and me, Applicant stated he only viewed pornography on the desktop computer and the pornography migrated to the two laptops because they were connected on the internal network. He stated he never viewed pornography on the company or Government laptops and did not know until after the laptops were analyzed that the pornography had migrated to those computers. (Tr. 101-104, 111-119, 123-130)

The pornographic websites had various viruses in them which caused the Government computer network that he was connected to and working on to be infected. He never received instruction on what he could or could not do with the computers until he was terminated. He was not initially told the computes could not be used for personal business or that unauthorized software could not be loaded. He was never told he could not download software onto the computers even if the software was to enable him to do his job better for the company and the Government. He believed it was common practice in the company to download software onto the laptop computers to enable the employees to better do their job. He testified that it was common knowledge that you could not use the company or Government computers to view or download pornography. He was not provided a copy of the company policy concerning the use of unauthorized software until the day he was terminated. (Tr. 43-47; Response to SOR, dated June 21, 2011, at 2)

Applicant was required to bring the work-related computers into the information systems security officer since viruses were discovered on the Government network and his computer was suspected of being the source of the virus. Prior to bringing in the computers, he used the antivirus software on the computers to look for and remove any viruses. He testified that he was told by the systems security officer to run the antivirus software before bringing the computer into the office. He informed the information systems security officer that he ran the antivirus software before turning in the computers. He did not tell him that he had viewed pornography from the Internet. (Tr. 47-49; Response to SOR, dated June 21, 2011, at 2-3)

Applicant has not viewed pornography since he was terminated in March 2009. He has received counseling concerning pornography from his pastor. He realizes the effect viewing pornography had on his family so he has stopped viewing pornography. (Tr. 61-64)

Applicant's co-worker testified that he has a computer program certificate and has been in the information technology business for over 30 years. He has worked as a web and database administrator for eight years at the company that fired Applicant. He has known Applicant for over six years both on the job and socially. At one time, Applicant was his supervisor. Applicant is very meticulous, structured, and detail oriented. He has never known Applicant to ignore rules or regulations. The co-worker never questioned Applicant's reliability, judgment, or sense of responsibility. He has no concerns about Applicant's managing classified information. (Tr. 18-23)

The co-worker is aware of the allegations against Applicant for loading unauthorized software onto the company computer. He testified that computer technicians like he and Applicant would try to find free and different software than provided on the computers to do their job correctly. The computer technicians would recommend to the Government agencies that certain software be standardized on the computers to assist them in doing the work for the agency. They were never told they could not load the non-standard software on the company or Government laptops. While he did not remember having specific instruction on what could be viewed on a company or Government laptop, it is common knowledge that pornography cannot be viewed or stored on either type of computer. The computer technicians received recurring training on the proper use of company or Government computers. (Tr. 23-26, 29-40)

The witness also testified that Applicant explained to him how he downloaded pornography on his home network and it migrated to the company and Government laptops. He believes that Applicant properly took action to resolve his problems with pornography. (Tr. 26-28)

Applicant's immediate supervisor for the last two years wrote that he has known Applicant for over nine years. Applicant is a valued member of their team and an extremely knowledgeable information technology professional. He is knowledgeable in many computer programs and applications and is their "go to" person. He highly recommends Applicant for access to classified information. (App. Ex. B, letter, undated)

Applicant's latest performance rating shows that Applicant achieved all of his goals and objectives. He demonstrates the understanding and commitment to the company's code of business conduct. His overall rating was that he meets or exceeds some goals. (App. Ex. C, Rating, dated June 15, 2011)

The facility security officer for Applicant's company wrote that he has known Applicant for over 18 months. Applicant is knowledgeable of the NISPOM and shows an understanding of security management of classified information. He has the required integrity, trustworthiness, and reliability to handle classified information. (App. Ex. D, Letter, dated June 20, 2011)

The Government employee that manages Applicant's program wrote that Applicant is one of the most knowledgeable persons in some computer programs and applications. She has been very impressed with his knowledge and understanding of the system. Applicant is a responsible responsive member of the team. (App. Ex. E, Letter, dated June 19, 2011)

An individual who worked with Applicant at his former place of employment for approximately seven years wrote that Applicant is meticulous, organized, and hardworking. He believes Applicant to be trustworthy, reliable, and he has no doubts about Applicant's ability to manage classified information. He understands the mistakes made by Applicant, but does not believe the mistakes reflect adversely on his ability to handle classified information. (App. Ex. T, Letter, dated October 31. 2011)

Applicant's testimony at the hearing concerning the viewing and downloading of pornography was different from the information he provided to security investigators and in his answer to the interrogatory. (Gov. Ex. 2, dated December 7, 2010). In both of these documents, he stated he used either the company or Government laptop to view the pornography. In his response to the SOR, Applicant stated he used the company computer to view the pornography. At the hearing, however, Applicant stated for the first time that he had a home internal network system with a personal desktop computer connected through a router to the two laptops. He stated he viewed the pornography on his personal desktop computer and the viruses in the pornography migrated to the laptops because the computers were connected. I find his testimony at the hearing not credible. It was common knowledge that viewing and downloading pornography on the company or Government computer was a violation of rules and regulations. However, it is not a violation of company or Government policy to view adult pornography on your own personal home computer. His testimony at the hearing was more favorable to him than the information he had previously provided. I find that his testimony was not credible and an attempt to put his actions in the most favorable position for him. Applicant's hearing testimony was so inconsistent from his previous testimony so that the only conclusion to be drawn is he failed to provide truthful and candid answers and information during the security clearance process.

Policies

When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the revised Administrative Guidelines. In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially disqualifying conditions and mitigating conditions, which are useful 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 access to classified information will be resolved in favor of 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. 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 burden of persuasion 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 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.

Analysis

Financial Considerations

Failure or inability to live within one's means, satisfy debts, and meet financial obligations may indicate poor self-control, lack of judgment, or unwillingness to abide by rules and regulations, all of which can raise questions about an individual's reliability,

trustworthiness, and ability to protect classified information. An individual who is financially overextended is at risk of having to engage in illegal acts to generate funds. (AG ¶ 18) Similarly, an individual who is financially irresponsible may also be irresponsible, unconcerned, or careless in their obligations to protect classified information. Behaving responsibly or irresponsibly in one aspect of life provides an indication of how a person may behave in other aspects of life.

A person's relationship with his creditors is a private matter until evidence is uncovered demonstrating an inability or unwillingness to repay debts under agreed terms. Absent evidence of strong extenuating or mitigating circumstances, an appellant with a history of serious or recurring financial difficulties is in a situation of risk inconsistent with the holding of a security clearance. An appellant is not required to be debt free, but is required to manage his finances in such a way as to meet his financial obligations. Appellant's delinquent debts, as established by a credit report, are a security concern. The evidence is sufficient to raise security concerns under Financial Considerations Disqualifying Conditions (FC DC) AG ¶ 19(a) (inability or unwillingness to satisfy debts), and (FC DC) AG ¶ 19(c) (a history of not meeting financial obligations). Appellant accrued delinquent debt when he was removed from his job and unemployed for over six months. He had sporadic employment thereafter for another six months. He was unaware that his health insurance did not cover all of his medical expenses and he incurred unpaid medical bills.

The case file provided sufficient evidence to establish the disqualifying conditions as required in AG ¶¶ 19(a) and 19(c). The burden is for Applicant to produce evidence to rebut, explain, extenuate, or mitigate the security concerns under financial considerations. The burden to refute an established allegation or prove a mitigating condition never shifts to the Government. Applicant raised conditions that may mitigate the security concern.

I considered Financial Consideration Mitigating Condition (FC MC) ¶ 20(a) (the behavior happened so long ago, was so infrequent, or occurred under such circumstances that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or good judgment), and FC MC ¶ 20(b) (the conditions that resulted in the financial problems were largely beyond the person's control (e.g. loss of employment, a business downturn, unexpected medical emergency, or a death, divorce, or separation) and the individual acted responsibly under the circumstances). These mitigating conditions apply. Applicant incurred delinquent medical debt because he was not aware that his health insurance did not pay all of his family medical expenses. The delinquent medical debts were small co-payments or expenses not covered by his company's health insurance program. Most of the bills were in his wife's name and he was unaware of them.

He also incurred delinquent debt when he was terminated from his job for misconduct in March 2009. He was unemployed for about six months and then had some employment for the next six months before finding permanent employment in April 2010. During the time of low or no employment, he used credit cards to meet expenses and also could not make his mortgage payments. Applicant acted responsibly to resolve

his delinquent debts. He paid or is paying his medical debts, has settled and paid his credit card debts, and his mortgage has been resolved by foreclosure. His past delinquent debts do not cast doubt on his current reliability, trustworthiness, or good judgment, since the delinquent debts are paid or being paid,

I considered FC MC AG ¶ 20(d) (the individual has initiated a good-faith effort to repay the overdue creditors or otherwise resolve debts). For FC MC AG ¶ 20(d) to apply, there must be an "ability" to repay the debts, the "desire" to repay, and "evidence" of a good-faith effort to repay. A systematic method of handling debts is needed. Good-faith means acting in a way that shows reasonableness, prudence, honesty, and adherence to duty or obligation. Applicant paid eight medical debts in full, disputed another, and has almost completed payment of the last medical debt. He paid a debt to a retail store in full, and settled and paid a credit card debt. He took reasonable action in attempting to resolve his mortgage issue. He could not pay his mortgage because of unemployment. The house lost value in the housing crisis and he could not sell it. He sought a mortgage modification or a short sale but was unsuccessful because the creditor did not agree. His house was foreclosed and resold by the mortgage company. He has no liability for the mortgages. He is current with his taxes and his current debts are being paid as agreed. He has sufficient discretionary income to meet his financial obligations. Applicant established that he adhered to his financial duty to resolve his delinquent debts by taking reasonable, prudent, and honest actions to resolve his debts. Since he is current with the payment of his bills and the delinquent debts in the SOR are resolved, he established a good-faith effort of debt resolution.

I considered AG ¶ 20(e) (the individual has a reasonable basis to dispute the legitimacy of the past due debt which is the cause of the problem and provides documented proof to substantiate the basis of the dispute or provides evidence of actions to resolve the issue). Applicant paid or is paying all but one of his delinquent medical debts. He tried but has not learned the origin of the unresolved debt. He contacted all of the medical facilities or providers that he and his family use but did not receive any billing information. When he has sufficient information, he will pay the debts. He has a basis for his dispute and has taken action to resolve the dispute. By acting responsibly towards his debts and establishing his debts are under control, Applicant presented sufficient information to mitigate security concerns for financial considerations.

Personal Conduct (Guideline E)
Use of Information Technology Systems (Guideline M)

The security concerns for personal conduct and use of information technology systems in this case are raised from the same incident. The security concerns for both, as well as the disqualifying conditions and mitigating conditions, are so similar that they will be discussed together. Personal conduct involving questionable judgment, untrustworthiness, unreliability, or unwillingness to comply with rules and regulations can raise questions about an individual's reliability, trustworthiness, and ability to protect classified information. Of special interest is any failure to provide truthful and candid answers during the security clearance process or any other failure to cooperate with the

security clearance process. (AG ¶ 15) Noncompliance with rules, procedures, guidelines, or regulation 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 ¶ 38)

Applicant was provided two laptop computers for his work by his employer. One computer was from the company, the other was from the Government agency his company supported. His employer and the Government agency found viruses in their database and traced the source to the computers provided Applicant. Applicant was required to bring in the computers for examination and analysis. Before bringing in the computers, he ran the antivirus software on the computers to erase any viruses. The computer review discovered that Applicant had loaded unauthorized software on the computers, and used the computers to view and download adult pornography. It was a violation of his company's and the Government agency's policy to load unauthorized software or view pornography on the computers. His actions in loading unauthorized software, viewing pornography, and attempting to erase the viruses raise personal conduct disqualifying condition AG ¶ 16(c) (credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any other single guideline, but which, when considered as a whole, supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristic that the person may not properly safeguard protected information); AG ¶ 16(e) (personal conduct, or concealment of information about one's conduct, that creates a vulnerability to exploitation, manipulation, or duress., such as (1) engaging in activities which, if known, may affect the personals professional or community standing …: and AG ¶ 16 (f) (violation of a written or recorded commitment made by the individual to the employer as a condition of employment. It also raises disqualifying conditions under use of information technology systems AG ¶ 40(e) (unauthorized use of government or other information technology system); and AG ¶ 40(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).

The case file provided sufficient evidence to establish the disqualifying conditions as required in AG ¶¶ 16(c), 16(e), 16(f), 40(e), and 40(f). Again, the burden is for Applicant to produce evidence to rebut, explain, extenuate, or mitigate the security concerns under use of information technology systems and personal conduct. The burden to refute an established allegation or prove a mitigating condition never shifts to the Government. Applicant raised conditions that may in part mitigate the security concerns

There is no question that Applicant downloaded software onto the company and Government provided laptops. There is also no doubt that it was against the company's and Government rules and regulations to download the software onto the laptops. However, Applicant and a witness testified that it was normal practice to load software

onto the laptops to assist them in performing their functions under the Government contract. Both men testified and established that they received no instructions directly from the company or the Government not to load the software unless authorized. In fact, there may be some tacit understanding that software could be loaded onto the computers and the company and Government informed to determine if it would be best to load the software as part of the normal process. He was not advised of the company policy until the day he was terminated. Applicant established that he did not knowingly violate the company and Government policy against loading unauthorized software because he believed the practice was permissible. He was instructed to run the antivirus software before returning the computers. It was not an attempt to hide his actions in regard to the unauthorized software or the pornography.

However, Applicant did not provide candid and truthful information concerning his violation of the rules against viewing pornography. He viewed the adult pornography on the company and Government computers, and not his personal home desktop computer. He was not truthful at the hearing when he testified that he did not view or download the pornography on his company or Government laptop in violation of the rule and regulations. I find against Applicant as to personal conduct and use of information technology systems for viewing and downloading pornography using either the company's or Government's laptop computers in violation of rules and regulations. I also find against Applicant as to personal conduct for not being truthful and candid in his testimony at the hearing.

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.

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. I considered that Applicant served four years on active duty in the Marine Corps and four years in the Marine inactive reserves. I also considered the testimony and opinions of Applicant's supervisors,

friends, and a co-worker as to his reliability, trustworthiness, and ability to manage classified information.

Applicant presented sufficient information to meet his burden to refute, explain, or mitigate the security concern for financial considerations. His loading of unauthorized software on the company and Government laptops was unknowing. However, he did not present sufficient information to refute, explain, or mitigate security concerns for personal conduct and use of information technology systems for viewing and downloading adult pornography on company and government laptops in violation of company and Government rules. At the hearing, he was not candid about his actions when he testified that he viewed the pornography on his personal desktop computer and not the company or Government laptops. He did not meet his burden to show his violation of the rules and regulations concerning use of information technology systems do not reflect adversely on his reliability, honesty, trustworthiness, and good judgment. For all these reasons, I conclude Applicant has not mitigated the security concerns for personal conduct and use of information technology systems. Overall, the record evidence leaves me with questions and doubts as to Applicant's judgment, reliability, and trustworthiness. Access to classified information is denied.

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
Subparagraph 1.a:	Against Applicant
Paragraph 2, Guideline E:	AGAINST APPLICANT
Subparagraph 2.a:	Against Applicant
Paragraph 3, Guideline F:	FOR APPLICANT
Subparagraphs 3.a – 3.m:	For Applicant

Conclusion

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

THOMAS M. CREAN
Administrative Judge