DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 10-03300
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Eric Borgstrom, Esq., Department Counsel
For Applicant: William Savarino, Esq.

August 11, 2011

Decision

RICCIARDELLO, Carol G., Administrative Judge:

Applicant failed to mitigate the Government's security concerns under Guideline M, Use of Information Technology Systems, and Guideline E, Personal Conduct. Applicant's eligibility for a security clearance is denied.

Statement of the Case

On October 27, 2010, the Defense Office of Hearings and Appeals (DOHA) issued Applicant a Statement of Reasons (SOR) detailing security concerns under Guidelines M and E. On March 2, 2011, DOHA issued an amendment to the SOR detailing additional security concerns under Guideline E. 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 within the Department of Defense on September 1, 2006.

Applicant answered the original SOR on November 15, 2010. He requested a hearing before an administrative judge. He answered the amendment to the SOR on the record at his hearing. The case was assigned to me on April 13, 2011. DOHA issued a Notice of Hearing on April 18, 2011. I convened the hearing as scheduled on May 23, 2011. The Government offered exhibits (GE) 1 through 7. Applicant did not object to those exhibits and they were admitted into evidence. Applicant and two witnesses testified on his behalf. He offered exhibits (AE) A through C, which were admitted into evidence without objection. DOHA received the hearing transcript (Tr.) on June 1, 2011.

Findings of Fact

Applicant admitted SOR ¶¶ 1.b, 2.a, and 2.b. He denied the remaining allegations. I incorporated his admissions into my findings of fact. After a thorough and careful review of the pleadings, exhibits, and testimony, I make the following findings of fact.

Applicant is 37 years old. He is married and has an eight-year-old son. He has worked for his current employer, a federal contractor, since June 2009. Prior to his present job, he worked for a different federal contractor from January 2003 to March 2009. He also worked part-time from 2000 to 2006, for a retail store, in their computer service department. He has a bachelor's and master's degree.[1]

In 1997, Applicant was working for a government agency and was laid off. He was in college at the time. He applied for unemployment insurance. He got a part-time job as a bartender. He was required to forecast his earnings and provide them to the unemployment agency. He occasionally earned more money than he forecasted because he often would not know how many hours he would be assigned to work. He did not go back to adjust the amount when he worked more hours than forecasted. He was required to report the amount he earned. He was informed by the state unemployment agency that he owed money to the state. He made full restitution. He was charged criminally with providing false information to the unemployment agency. He was represented by an attorney. He went to court and pled no contest to one charge of providing false information and the other charge was dismissed. He did not receive any jail time or punishment. Applicant did not disclose this offense on his 2002 security clearance application. He stated he did not know why he did not list it. He stated he did not think about the offense and forgot about it. He indicated he did disclose the offense when he was interviewed by an investigator in 2004 or 2005. He did not list the incident on his 2007 SCA because it was beyond the seven year time frame.[2]

While working part-time for a retail store from 2000 to 2006, Applicant and his computer expert colleagues would collaborate with each other and share computer applications and best practices in an attempt to arrive at resolutions for customers' computer problems. They would exchange software and information. Applicant stated

[1] Tr. 41-47,108.

[2] Tr. 88-102, 109-123.

he never copied any software from his full-time or part-time employers. He would legally download shareware and free software, copy it to a compact disc, and share it with his colleagues. Applicant stated he never duplicated copyrighted material from his employers.[3]

Due to his expertise in computers, Applicant's friends would ask him to build computers for them. They would supply him with the hardware and the software. He built computers for a few friends from 2001 to 2004. He would install software that was given to him by his friends. He did not inquire if the software was obtained legally. He admitted that some of the software could have been illegally obtained. When he was later polygraphed, he admitted that he thought some of the software might have been "hinky" so he disclosed it to the polygraph examiner. He stated he did not question the legality of the software unless he did not have "the key" required to open the software. He got the "key" from the internet. He stated he found the "key" for the majority of the software he was looking for by searching the internet. He admitted he should have questioned whether the software was legally obtained. I find Applicant was aware that some of the software he used was not legally purchased and he was aware that by obtaining the "key" from the internet he was illegally downloading the programs.[4]

Applicant admitted he copied some DVDs that he rented from Netflix. In his answer to the SOR, he stated:

> In the fall of 2003, I made copies of <u>at most</u> five DVDs I had rented from Netflix. I viewed these copies as backups solely for my personal use and I never sold or otherwise distributed them. After thinking more critically about my actions, I concluded that copying the rented DVDs was not right. I immediately stopped copying all DVDs and subsequently threw out all of the copied DVDs I had made.[5]

He stated at his hearing that the reason he copied the DVDs was because one time he had broken a DVD and Netflix made him pay the purchase price for the DVD. He then started backing up the DVDs just in case it happened again. He did this prior to 2004. While working at the retail store in 2004, he learned that copying DVDs was illegal. He believed this was based on a new law that was passed in 2004. He never copied DVDs after 2004, although his brother continued to do so. He did not tell his brother to stop. He admitted to watching the DVDs that his brother copied, but he did personally copy any more.[6]

[3] Tr.81-88, 128-140.

[4] Tr. 77-81, 140-144.

[5] Answer to SOR.

[6] Tr. 123-128.

In October 2004, Applicant admitted to a government investigator that he downloaded about 100 to 150 songs to an MP3 player from 1996 to 2002. He said about 90% were downloaded before he left college. He was in college from 1991 to 1999, earning his bachelor's and master's degree. He stated this occurred during a time when online sharing of music was widespread and the legality of the activity was still controversial. When he left school he downloaded about 10 to 20 songs between 1999 and 2002. When it became clear that this was a violation of copyright laws in 2002, he immediately stopped his actions. He has not illegally downloaded any music to MP3 players or other devices since early 2002.

Applicant also admitted he disclosed to a government investigator that he copied legal MP3 files and CDs to his corporate computer for the purpose of importing them into iTunes and listening to them during non-work hours. He stated he never downloaded music from the Internet to his corporate computer. He stated the copying of music files is not a violation of his employer's internet policy which prohibits the downloading of music files from the internet.[7]

Applicant admitted he knew he was downloading software that was copyrighted and that was not free or a trial version. He would get the key from the Internet, install the program, and decide whether to purchase the program. He admitted he wrongfully obtained the key to make the program work. Applicant knew he was not authorized to use the software and that he was violating the licensing requirement by using an unauthorized key he obtained.[8]

Applicant admitted that he took a copy of Turbo Tax software that he copied onto a compact disk, brought it to work and put it on his work laptop computer. He originally obtained the copy of Turbo Tax to use for free for a 30-day trial period. He obtained the program from an unofficial Internet site that had a "key" to unlock it. He used it past the 30-day trial period. He stated that he was deciding whether to buy Turbo Tax or another comparable tax software program, so he wanted to check it out. He inserted the compact disk into his work laptop computer. His laptop computer automatically scans the disk for viruses. He took his work laptop home and estimated the Turbo Tax program remained on the computer for a few days. He did not use his personal computer to load Turbo Tax because his computer was old and it did not have a lot of memory. I find Applicant loaded unauthorized software on his corporate computer system.[9]

Applicant admitted that he obtained a copy of Norton Utility software from the Internet. He brought it to work and used it on his work computer because it had a more

[7] Tr. 71.

[8] Tr. 128-139. It is unclear exactly what year Applicant downloaded the software, but it appears it was prior to his denial of a security clearance by a government agency in March 2006.

[9] Tr. 62-68, 150-155; AE C is a statement made by Applicant in March 2006. He admitted to installing an unauthorized version of Turbo Tax on his work computer,

advanced anti-virus program than the one his employer used. His employer did not have Norton Utility. His work computer ran the program from the compact disks he inserted into it. He did not think to ask for authorization from his employer to use it on his work computer. I find Applicant used unauthorized software on his corporate computer system.[10]

Applicant stated that his employer's policy was that employees could use their work computer for personal use as long as they adhered to the company's standards and they were not billing their time to a contract. Applicant stated he disclosed the above mentioned uses during a polygraph examination. He stated that other employees were doing the same thing he was doing. He was never disciplined by his employer. He stated an employee did not need authorization from the employer to use work computers for personal purposes or to run programs that were not provided by the employer. He stated employees were allowed to use other disks as long as they were scanned for viruses. He stated they were also allowed to use software not provided by the employer, provided it was first scanned.

Applicant admitted to copying other software from the Internet. He did not pay for the software, which was required. He would test it on his work computer, so he could decide whether or not he wanted to purchase it. He then paid for the software that he wanted to retain. He did not pay for the software he decided not to retain. Unlike Turbo Tax, these programs did not offer a free trial period. Applicant knew his actions were illegal. He admitted what he did was wrong, but stated he purchased some of them later. He admitted he needed a special key to access some of the programs to make them work. He obtained the key from the Internet to run the programs. He was not authorized access to the key.[11]

In a March 2006 letter appealing the denial of a security clearance by another government agency, Applicant stated:

> Most of the software I "acquired" by downloading was freeware or trial versions that expired after a couple of weeks. The only software that I downloaded that were not free or trial versions were Windows XP ($199), Windows 98 ($50), Windows 2000 ($120), Norton Antivirus ($29), Microsoft Office ($149), Norton Systems Works ($48), Turbo Tax ($30), and EZ Creator ($79). At the time of my interview, I stated that this software was worth between $2,000 and $3,000. This was an incorrect statement. The [actual] value of the software was not more than $705.
>
> In some cases, I used keys available on the [I]nternet to install the software. I downloaded this software to test their functionality before buying the product. After previewing the software, I purchased the ones that I needed (Windows XP, Norton Antivirus, Turbo Tax, and Microsoft

[10] Tr. 68-71, 158-159.

[11] Tr. 55-56, 72-77; AE C.

> Office) and completely uninstalled and erased the others (EZ CD Creator). Copies of the receipts for the software I purchased are attached. Looking back, I realize now that I should not have used keys obtained from the [I]nternet to install the products prior to actually purchasing them.[12]

As part of his job, Applicant worked inside a lab with computers. The area did not have Internet connectivity. Any research that was conducted had to be completed outside of the lab spaces. On occasion, Applicant had to test software that was on the network server. He copied the software to his work laptop and tested it to make sure it worked. He would then remove it from the work laptop after the testing was complete. These tasks were part of his work responsibilities. He stated he did not need authorization from his employer to do this testing.[13]

The employer's corporate procedures state:

> Prohibited Activities and Conduct
>
> Violations of the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of pirated or other software products that are not appropriately licensed for use by [employer].
>
> Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted software sources; copyrighted music; and the installation of any copyrighted software for which [employer] does not have an active license.
>
> * * *
>
> Downloading and/or installing any software without authorization, unless it is a part of a job requirement. Such action could:
>
> -infringe intellectual property rights of a third party.
> -introduce vulnerabilities, viruses, and spyware into the company's IT network.
> -cause operational systems to cease operating correctly.
>
> Files prohibited from Internet downloading are:
>
> -music
> -entertainment videos

[12] AE C.

[13] Tr. 55-61, 146-150.

-games
-screen savers

* * *

Data files, such as documents, spreadsheets, presentations, pictures, audio, and video, are only permitted for Internet downloading if they:

-have been checked for viruses.
-are business relevant.
-do not infringe on copyright laws.
-are not otherwise prohibited by this procedure.[14]

Applicant installed iTunes on his work computer. He believed he was authorized to do so. His employer's policy prohibited installing the program. He stated he was aware he was not authorized to install Turbo Tax, but was unaware of the prohibition against iTunes because "everybody in [the company] had the software on their computer."[15]

In 2007, Applicant was interviewed by a government investigator. He advised the investigator that he had been previously denied a security clearance. He testified that he told the investigator he did not know the specific reasons why he was denied the clearance by another government agency. He told the investigator that he was not accused of any wrongdoing and that he was simply told by the agency that he was not a good candidate and no further details or explanations were provided to him. He appealed the denial and was represented by counsel. He provided a 16-page letter with enclosures to the agency in support of his appeal. He told the investigator that he never received a final decision on his appeal. At his hearing, he admitted he had received a letter from the agency before he was interviewed, advising him of the initial denial, but at the time of his interview, he did not recall the reasons for the denial.[16]

A letter dated March 10, 2006, to Applicant from the government agency detailed the reasons he was denied a security clearance. It stated Applicant's personal conduct was the reason for the denial. It specifically stated Applicant's disclosure of his criminal charge for providing false information to obtain unemployment benefits; his admissions to downloading MP3 files and copying DVDs; building computers for friends and installing illegally downloaded software; and copying software as the reasons for the denial.[17]

[14] Tr. 154-156; AE C, Tab C.

[15] Tr. 156-158.

[16] Tr. 103-107, 159-174; GE 5, 6, 7.

[17] Tr. 51-53; GE 5, 6.

When asked why he told the government investigator that he was denied program access because he was not a good candidate and failed to disclose the content of the denial letter, he stated he could not recall the details of the letter. He indicated that his interview statements included in his interrogatory were somehow out of context, but he did not correct them when they were provided to him. He did not know why he made the statement to the investigator. At his hearing, he admitted he was denied a security clearance by the government agency due to personal conduct. Applicant's testimony was not credible. I find he intentionally misled the government investigator by providing false information.[18]

A former coworker testified on behalf of Applicant. He worked with Applicant when they both worked for two different employers in about 2001 through about 2004. They have maintained a personal relationship since then, but they no longer work together. Their first employment together was for a small company. The witness stated there were certain inherent rules for safeguarding data and security within the company. When they worked for a larger company, there were written rules. The witness was unaware of any infractions committed by Applicant. The witness trusted Applicant and was not aware of him being dishonest or breaking rules. He indicated that there was annual mandatory security training provided by their employer.[19]

Another witness who worked with Applicant in 2004 testified on his behalf. They worked together for about 18 months. They maintained a personal relationship after they no longer worked together. He could not recall the security rules or information technology rules at the company where they worked. He was not aware of Applicant committing any infractions. He believes Applicant is trustworthy and dependable. He commented that Applicant would remind him to follow certain procedures.[20]

Applicant provided a character letter from a coworker. She has known him since 1992 when they met at college. They later worked together on two projects, one in 2001 for about six months and again in 2007 for about 18 months. She believes Applicant to be honest, trustworthy, ethical, dependable, add a person of high character. To her knowledge, he follows the rules of employment both with regards to internal operations and clients. She stated: "[Applicant] told me that the issues identified in the Statement of Reasons are behind him and I believe him based on my experiences with him over the last several years."[21]

Another character letter was provided from his college roommate. He has known Applicant since 1994. He considers Applicant a hard-working and trustworthy person.

[18] Tr. 103-107, 159-174; GE 5, 6, 7. The final denial letter in response to Applicant's appeal was issued on January 10, 2010.

[19] Tr. 18-29.

[20] Tr. 29-40.

[21] AE A.

He is punctual and works long hours to fulfill his work obligation. He follows the rules of employment. He "previously and presently has access to company proprietary, classified or export controlled data under an obligation not to disclose such protected information." He indicated that Applicant follows the rules regarding sensitive, proprietary, and classified material.[22]

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 are used in evaluating an applicant's eligibility for access to classified information.

These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, these guidelines are applied in conjunction with the factors listed in the adjudicative process. The administrative judge's overarching adjudicative goal is a fair, impartial, and commonsense decision. According to AG ¶ 2(c), the entire process is a conscientious scrutiny of a number of variables known as the "whole-person concept." The administrative judge must consider all available, reliable information about the person, past and present, favorable and unfavorable, in making a decision.

The protection of the national security is the paramount consideration. AG ¶ 2(b) requires that "[a]ny doubt concerning personnel being considered for 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, an "applicant is responsible for presenting witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by applicant or proven by Department Counsel and has the ultimate burden of persuasion 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

[22] AE B.

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 as to the loyalty of the applicant concerned." *See also* EO 12968, Section 3.1(b) (listing multiple prerequisites for access to classified or sensitive information).

Analysis

Guideline M, Use of Information Technology Systems

AG ¶ 39 expresses the security concern pertaining to use of information technology systems:

> Noncompliance with rules, procedures, guidelines, or regulations pertaining to information technology systems may raise security concerns about an individual's reliably 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 describes conditions that could raise a security concern and may be disqualifying. I find two are potentially applicable:

> (e) unauthorized use of a government or other information technology system; and
>
> (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.

Applicant installed and illegally downloaded software when he built computers for his friends. He illegally downloaded software, used it, and purchased it if he decided to keep it; otherwise he would remove it from his computer. He did this to screen the software and circumvent having to pay for it before he decided he wanted it. He downloaded at least two programs (Turbo Tax and Norton Utility) on his work computer in violation of company rules. He illegally copied MP3 music files and DVDs. I find the above disqualifying conditions apply to these facts.

There is insufficient evidence to conclude that Applicant removed software from his corporate computer without authorization, as alleged in SOR 1.c, or that he copied software from two places of employment, as alleged in SOR 1. b.

I have considered all of the mitigating conditions under AG ¶ 41 and three 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.

I did not find Applicant's testimony credible. He is very knowledgeable about information technology. He was aware that, absent a manufacturer's trial offer, he was required to pay for software before he used it. I did not find his testimony credible when he said he did not know if the software his friends gave him was legally purchased. I find he knew that when he had to search for a "key" on the Internet to access the software, he knew it was pirated software. Applicant did not have authorization to use his work computer to download Turbo Tax so he could test it. He did not have authorization to download Norton Utility on a company computer without a license. By doing so, he violated his company's rules. The downloading of music files and copying DVDs were minor infractions and based on when they happened, it is possible that Applicant did not realize his actions were illegal at that time. However, he has exhibited a continuing course of conduct in bypassing and circumventing the rules. His actions cast doubt on his trustworthiness and good judgment. His actions were intentional and are not considered minor. I find none of the above mitigating conditions apply.

Guideline E, Personal Conduct

AG ¶ 15 expresses the security concern pertaining to personal conduct:

> Conduct involving questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations can raise questions about an individual's reliability, trustworthiness, and ability to protect classified 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 ¶ 16 describes disqualifying conditions that could raise a security concern. The following is potentially applicable:

(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, awarded benefits or status, determine security clearance eligibility or trustworthiness, or awarded fiduciary responsibilities;

(b) deliberately providing false or misleading information concerning relevant facts to an employer, investigator, security official, competent medical authority, or other official government representative;

(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 person's personal, professional, or community standing.

Applicant failed to disclose he was charged with providing false information to obtain unemployment benefits. He pled no contest to one charge and paid restitution. I find his failure to disclose his criminal offense was not inadvertent, but deliberate. Applicant made a false statement to a government investigator during his security interview when he stated he was not accused of any wrongdoing or given an explanation as to why another government agency denied him a security clearance. Applicant's explanations lacked candor and were not credible. I find he intentionally and deliberately provided false information to a government investigator. Applicant illegally downloaded software, obtained keys to use the software, used his computer expertise to bypass copyright laws, and violated company rules. I find the above disqualifying conditions apply.

I have considered all of the mitigating conditions under AG ¶ 17 and the following four are potentially applicable:

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

(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 caused untrustworthy, unreliable, or other inappropriate behavior, and such behavior is unlikely to recur; and

(e) the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress.

Applicant was represented by an attorney when he pled no contest for providing false information to the unemployment agency. I did not find him credible that he forgot about the offense when he failed to disclose it on his security clearance application. Applicant's statement to the government investigator that he was told he was not a good candidate for the job and it had nothing to do with any wrongdoing, as the reason he was previously denied a security clearance, was a false and misleading statement. Applicant was provided a written explanation regarding his wrongful actions as the reason he was denied a security clearance. He provided a 16-page appeal to the denial. His explanation that he could not recall why he was denied is not believable. I find he intentionally and deliberately provided false and misleading information to the investigator. Applicant's conduct exhibits a pattern of untruthfulness and raises serious security concerns. My conclusions under Guideline M apply equally under Guideline E, regarding Applicant's personal conduct. Applicant's repeated serious misconduct casts doubt on his reliability, trustworthiness, and good judgment. Although Applicant acknowledges some of his behavior was wrong, I did not find his testimony credible, and therefore cannot conclude his behavior is unlikely to recur, or that he has reduced his vulnerability to exploitation, manipulation or duress. Therefore, I find none of the mitigating conditions apply.

Whole-Person Concept

Under the whole-person concept, the administrative judge must evaluate an applicant's eligibility for a security clearance by considering the totality of the applicant's conduct and all the circumstances. The administrative judge should consider the nine adjudicative process factors listed at AG ¶ 2(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 have incorporated my comments under Guidelines M and E in my whole-person analysis. Some of the factors in AG ¶ 2(a) were addressed under that guideline, but some warrant additional comment. Applicant is well respected by his community of coworkers. He is intelligent and an obvious expert in the field of information technology systems. Early in his career and during a time when the computer music business was new and not well regulated, he

downloaded music that, at that time, he likely did not think he was required to pay for. Later, as he became more familiar with the industry, he took advantage of his expertise and obtained software and keys to unlock the software without paying for it. He built computers for his friends and was aware that some of the software was illegally obtained, which required a search of the Internet to find the key to unlock it. It appeared to be somewhat common practice to listen to iTunes on his employer's computer, which is a minor infraction. However, he also used software that was not authorized on his employer's computer, in violation of company rules. He circumvented the process for purchasing software because he was able to use his expertise to bypass the process. Although he later paid for some of the software, it does not negate or minimize his violations. Many of these issues were revealed when he was subjected to a polygraph. Applicant was denied a security clearance by another agency, which is not a disqualifying condition. He appealed the denial, but his false statements to a government investigator during his security clearance interview are the cause of concern. His past criminal offense for obtaining unemployment benefits is not significant by itself, but when considered with the other falsification issues that were raised, and the fact that Applicant failed to disclose the offense, it raises security concerns. Overall, the record evidence leaves me with questions and doubts about Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude Applicant failed to mitigate the security concerns arising under the guidelines for Use of Information Technology Systems and Personal Conduct.

Formal Findings

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

Paragraph 1, Guideline M:	AGAINST APPLICANT
Subparagraph 1.a:	For Applicant
Subparagraph 1.b:	Against Applicant
Subparagraph 1.c:	For Applicant
Subparagraph 1.d:	Against Applicant
Paragraph 2, Guideline E:	AGAINST APPLICANT
Subparagraph 1.a:	For Applicant
Subparagraph 1.b:	Against Applicant
Subparagraph 1.c;	Against Applicant
Subparagraph 1.d:	Against Applicant
Subparagraph 1.e:	Against Applicant

Conclusion

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

_____
Carol G. Ricciardello
Administrative Judge