DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 10-08589
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Raashid Williams, Esquire, Department Counsel
For Applicant: *Pro se*

03/26/2012

Decision

LYNCH, Noreen A., Administrative Judge:

After a review of the pleadings, exhibits, and testimony, I have questions and doubts as to Applicant's eligibility and suitability for a security clearance, as he has not mitigated the Government's security concerns. Applicant's eligibility for access to classified information is denied.

Applicant signed an Electronic Questionnaire for Investigations Processing (e-QIP) version of a security clearance application (SF-86) on January 21, 2010. The Defense Office of Hearings and Appeals (DOHA) issued Applicant a Statement of Reasons (SOR) that is undated, detailing security concerns under Guideline E (Personal Conduct), and Guideline M (Use of Information Technology Systems), that provided the basis for its preliminary decision to deny him a security clearance. 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 For Determining Eligibility for Access to Classified Information* (AG) implemented on September 1, 2006.

Applicant answered the SOR in writing on September 27, 2011, and requested a hearing on the record. The Government requested a hearing before an administrative judge. I received the case assignment on February 21, 2012. DOHA issued a notice of hearing on February 24, 2012, and I convened the hearing as scheduled on March 15, 2012. The Government offered four exhibits marked as GE 1 through 4, which were admitted into evidence without objection. Applicant testified. He did not submit any documents. DOHA received the transcript of the hearing (Tr.) on March 23, 2012.

Findings of Fact

In his Answer to the SOR, Applicant admitted the factual allegation in ¶ 1.b, and denied the other allegations in the SOR. His admission is incorporated herein as a finding of fact. After a complete and thorough review of the evidence of record, I make the following additional findings of fact.

Applicant is 59 years old. He received his undergraduate degree in 1974. Applicant earned a graduate certificate in August 2007. Applicant is married and has two children. He has held a security clearance since 1994. Applicant has worked for his current employer since 1994. (GE 1)

In 1999, Applicant used unclassified media in a classified computer system. He disclosed this information in his 2010 security clearance application. Applicant stated this was an isolated incident. He received a reprimand for the security violation. (GE 1; Tr. 17) Applicant told the investigator in 2010 that he was originally told it was "ok" to insert the unclassified disk into a classified computer. (GE 3)

Applicant acknowledged that as late as August 2009, he occasionally downloaded software such as drivers, evaluation software, and programming tools, that he would use when performing his engineering work. (GE 2) He stated that since 1994, he has downloaded software that was not available on the company network to help with his work approximately 30 to 40 times. In fact, Applicant answered "yes" to Section 27: Use of Information Technology, question (c) that he used hardware, software or media in connection with any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines, or regulations. (GE 1) He maintained that this was always on an unclassified system.

At the hearing, Applicant explained that he denied the allegation concerning the downloading of unclassified information due to the wording of SOR allegation 1.a. He believes he did not do so every month from 1994 until the present, but he admits there were about 40 occasions. In his DOHA interrogatories he explained that he downloaded software needed in order to do his engineering work on some jobs. He downloaded software that was not available on the work network. The software was needed to operate laboratory hardware or to do data collection and analysis or research. (GE 2)

When questioned about the company policy, Applicant was vague. He knew there was a policy and had also received emails concerning the policy. He admitted that he violated company policy when he downloaded the software that was not available

through work. He said there was an understanding that he was not supposed to do that, but other people did it. He stated that he did not always get explicit authorization, but on a few occasions his manager told him to do it. (Tr. 23) He never had written permission, but believed he had verbal authority a few times.

Applicant testified that he knows the difference between using unclassified and classified computer systems. He elaborated that he follows the rules on classified systems. He stated there is always a systems administrator, if he has questions. He also states that the fact that he has downloaded software on an unclassified system is not a factor in denying him his clearance. (Tr. 10) However, at the hearing, Applicant admitted that as late as 2009, he would download software and he understood that it was something he was not supposed to do. (Tr. 54) He also acknowledged that he never bothered to ask for clarification or guidance on this issue. (Tr. 55)

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.

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. . . ." An applicant has the ultimate burden of persuasion for 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 an 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.

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 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 describes the disqualifying conditions that could raise security concerns. I have considered all the conditions, and especially the following: (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, procedure, guidelines or regulations; and (g) negligence or lax security habits in handling information technology that persist despite counseling by management.

Applicant admitted that from approximately 1994 until the present he downloaded software, including drivers, programming tools and evaluation software approximately 30 to 40 times without following appropriate authorization procedures. He also received a citation for a security violation in 1999 for using unclassified media in a classified computer system. Applicant's actions are a violation of the policies and regulations regarding the misuse of government-issued information technology equipment. The Government has established a *prima facie* case under Guideline M.

AG ¶ 41 provides conditions that could mitigate security concerns:

> (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 admitted 2009 instance of downloading software in an unclassified system without appropriate authorization procedures is recent. Applicant does not accept any responsibility for his actions. He knows he did not have authorization for the many times (40) since 1994 that he downloaded the software. He states that it helped his work, but he knew it was against policy. Applicant refers to the fact that other engineers did the same thing. He admitted that he never actually checked the policy. He has no insight into his behavior. He did not act reasonably under the circumstances. His misconduct casts doubt on his current reliability. His conduct is not mitigated under AG ¶ 41(a), (b), or (c).

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 the disqualifying conditions that could raise security concerns. I have considered all the conditions, and especially the following:

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

(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 characteristics indicating that the person may not properly safeguard protected information;

(d) credible adverse information that is not explicitly covered under any other guideline and may not be sufficient by itself for an adverse determination, but which, when combined with all available information supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the person may not properly safeguard protected information. This includes but is not limited to consideration of:

(1) untrustworthy or unreliable behavior to include breach of client confidentiality, release of proprietary information, unauthorized release of sensitive corporate or other government protected information:

(2) disruptive, violent, or other inappropriate behavior in the workplace;

(3) a pattern of dishonesty or rule violations; and,

(4) evidence of significant misuse of Government or other employer's time or resources;

(e) personal conduct, or concealment of information about one's conduct, that creates a vulnerability to exploitation, manipulation, or duress, such as (1) engaging in activities which, if known, may affect the person's personal, professional, or community standing, or (2) while in another country, engaging in any activity that is illegal in that country or that is legal in that country but illegal in the United States and may serve as a basis for exploitation or pressure by the foreign security or intelligence service or other group; and

(f) violation of a written or recorded commitment made by the individual to the employee as a condition of employment.

Applicant violated the work policy by downloading software without appropriate authorization from 1994 until the present. He also admitted to his 1999 security violation in a classified system. He exercised poor judgment by not checking the policy or obtaining express permission for each use. His behavior was not appropriate. Applicant does not believe that his behavior should affect his ability to handle classified

information. He produced no documentation to show that he had guidance from any manager or specific permissions for his actions. AG ¶¶ 16(d) 2 and 16(d) 3 apply.

AG ¶ 17 provides conditions that could mitigate security concerns:

> (a) the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts;
>
> (b) the refusal or failure to cooperate, omission, or concealment was caused or significantly contributed to by improper or inadequate advice of authorized personnel or legal counsel advising or instructing the individual specifically concerning the security clearance process. Upon being made aware of the requirement to cooperate or provide the information, the individual cooperated fully and truthfully;
>
> (c) the offense is so minor, or so much time has passed, or the behavior is so infrequent, or it happened under such unique circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment;
>
> (d) the individual has acknowledged the behavior and obtained counseling to change the behavior or taken other positive steps to alleviate the stressors, circumstances, or factors that caused untrustworthy, unreliable, or other inappropriate behavior, and such behavior is unlikely to recur;
>
> (e) the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress;
>
> (f) the information was unsubstantiated or from a source of questionable reliability; and
>
> (g) association with persons involved in criminal activity has ceased or occurs under circumstances that do not cast doubt upon the individual's reliability, trustworthiness, judgment, or willingness to comply with rules and regulations.

Applicant's conduct is not mitigated. He violated policy for many years. He acknowledged his behavior as late as 2009. He states that what he did by not getting express authorization for downloading on an unclassified system has nothing to do with his ability to handle classified information. He admitted a 1999 security violation. He has shown poor judgment over many years. His serious misconduct casts doubt on his reliability and trustworthiness. He has not mitigated the personal conduct 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 an applicant's conduct and all relevant 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. The decision to grant or deny a security clearance requires a careful weighing of all relevant factors, both favorable and unfavorable. In so doing, an administrative judge must review all the evidence of record, not a single item in isolation, to determine if a security concern is established and then whether it is mitigated. A determination of an applicant's eligibility for a security clearance should not be made as punishment for specific past conduct, but on a reasonable and careful evaluation of all the evidence of record to decide if a nexus exists between established facts and a legitimate security concern.

In reaching a conclusion, I considered the potentially disqualifying and mitigating conditions in light of all the facts and circumstances surrounding this case. Applicant has worked as an engineer for many years. He has held a security clearance since 1994. He obtained a graduate certificate in 2007.

Applicant admitted that he received a security citation in 1999. He is firm that this was an isolated incident. However, from 1994 until the present, he has downloaded software onto his unclassified system. He did this to help him with his work, but he acknowledged that it was against policy. He does not believe that what he has done has anything to do with handling classified information. He has not shown candor or accepted responsibility for his behavior. This is serious and spans a long period. He has no insight into his behavior. He does not accept responsibility for the behavior.

Overall, the record evidence leaves me with questions and doubts as to Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude Applicant has not mitigated the security concerns arising from his misuse of information technoloy under Guideline M and his personal conduct under Guideline E.

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
Subparagraph 1.b:	Against Applicant
Paragraph 2, Guideline E:	AGAINST APPLICANT
Subparagraph 2.a:	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 eligibility for a security clearance. Eligibility for access to classified information is denied.

Noreen A. Lynch
Administrative Judge