DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 11-02847
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Ray Blank, Esq., Department Counsel
For Applicant: *Pro se*

02/29/2012

Decision

HEINY, Claude R., Administrative Judge:

Applicant was terminated from one job in January 2006 and from another in July 2009. Applicant has rebutted or mitigated the security concerns under use of information technology systems and personal conduct. Clearance is granted.

History of the Case

Applicant contests the Department of Defense's (DoD) intent to deny or revoke his eligibility for an industrial security clearance. Acting under the relevant Executive Order and DoD Directive,[1] the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) on August 8, 2011, detailing security concerns under Guideline M, Use of Information Technology Systems.

[1] Executive Order 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; Department of Defense (DoD) Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the adjudicative guidelines (AG) effective within the DoD on September 1, 2006.

On August 21, 2011, Applicant answered the SOR and requested a hearing. On October 5, 2011, I was assigned the case. On October 7, 2011, DOHA issued a Notice of Hearing for the hearing held on October 24, 2011.

The Government offered exhibits (Ex.) 1 and 2, which were admitted into evidence without objection. Applicant testified on his own behalf. The record was held open to allow Applicant to submit additional information. On November 8, 2011, additional material was submitted. Department Counsel had no objection to the material, which was admitted into the record as Exs. A through E. On November 2, DOHA received the hearing transcript (Tr.).

Motion to Amend SOR

At the close of the evidence, Department Counsel moved to amend the SOR by requesting the same allegations be considered under Guideline E, Personal Conduct. (Tr. 63) The motion was granted. (Tr. 65) The new guideline was not specifically added as paragraph 2.

Findings of Fact

In Applicant's Answer to the SOR, he admitted the two factual allegations in the SOR, and his admissions are incorporated herein. After a thorough review of the pleadings and exhibits, I make the following findings of fact.

Applicant is a 67-year-old systems administrator, who has worked for a defense contractor since June 2010. In 1983, Applicant began working with a company. (Tr. 20) The company ownership changed several times, but he continued to do the same job. (Tr. 20) There were periods of time when he worked for other employers, but would return to this employer. (Tr. 30, 31) The company employed about 350 people. (Tr. 35)

In July 1995, Applicant reached his ten-year anniversary with his employer. (Exs. B, C) The company's president indicated Applicant, as a software developer, had been a major contributor to the company's growth. In July 2005, he received an award for twenty years of service. (Ex. E) The accompanying letter cited Applicant as being a major contributor to the company's achievements, his skills as a software developer as being crucial in the development of test tools, and his work performance outstanding. (Ex. D) He was called upon daily to isolate and resolve user issues.

In December 2005, Applicant was trying out a new protocol at his government workstation when he accessed a "peer-to-peer" web site. The company prohibited employees going to "peer-to-peer" sites. (Tr. 33) In "peer-to-peer" computing or networking, one computer will connect or contact two or more computers in order to download or upload information. (Tr. 21) It is a distributed application that partitions tasks or workloads among peers. All the machines attempt to fill in parts of missing information. (Tr. 21) Peers are equally privileged participants in the application. Peers make a portion of their resources, such as processing power, disk storage or network

bandwidth, directly available to other network participants, without the need for central coordination by servers or stable hosts. The security concern is the other computers may be infected. There is no way of knowing about the other computers, the status of their antivirus or anti-spam ware programs, how to monitor the other machines, if they are secure, or if they are a threat to other computers. (Tr. 22)

Within a workday, he was told to unplug his computer and stay off the network. (Tr. 34) Two work days later, in January 2006, he was terminated from his employment as a systems administrator. (Tr. 35) He was not given an opportunity to explain what had happened. (Tr. 35) He asserts his action was unintentional. (Tr. 21) There were no labels and no warning that the site he was going to was a "peer-to-peer" site. (Tr. 33)

Applicant admits going to the unauthorized site, regrets that he did, asserts it will not happen again, and asserts it was not caused by lax security habits. (Tr. 73) He no longer goes to such sites even on this home computer. (Tr. 22)

At the time of his termination, he was one of the highest-paid non-management employees in the company. (Tr. 51) The income of newly hired employees, those just out of school, was less than half of his salary. (Tr. 52) He was 62 years old when terminated. While employed for the company, he was aware that other employees had gone to inappropriate web sites and were reprimanded, while others had their employment terminated. (Tr. 51) He could not say if his age or salary played a role in the company's decision to terminate him. (Tr. 52) His current job pays slightly more than the job from which he was terminated. (Tr. 56)

After his termination, he mowed lawns and repaired cars and computers for about 14 months before he got a job as a system administrator. (Tr. 37) That job lasted five months. (Tr. 23) From September 2007 to July 2009, Applicant worked as an information assurance security officer for a small contractor employing seven people that supported 350 military personnel. (Tr. 27, 28) The job entailed setting up computers, diagnosing problems, trouble-shooting, upgrading machines, and keeping records. (Tr. 24, 26)

Initially, he interacted well with the unit's commander and executive officer, an active duty lieutenant colonel and a major. A new lieutenant colonel became commander, and two months thereafter, a new major took over. The new major complained about Applicant to the point his company tried to find him a new position. When that failed, he was let go and received unemployment compensation. (Tr. 25) The major never gave him any indication there was a problem. (Tr. 41) He maintained a good relationship with the commander. (Tr. 41) The company never provided an explanation or reason for his termination. (Tr. 42) He received no written information from the company. (Tr. 43)

The state has traditionally recognized the employee "at will" doctrine, meaning that an employee works and a business employs on an "at will" basis. Under this doctrine, either may cease the employment relationship without cause at any time. (Tr. 42) Cause for termination is not required. Applicant indicated his termination was "for

cause." He referred to that phrase as a catch-all. Not having a more specific reason for his termination and not knowing how to describe his termination, he stated it was "for cause." (Tr. 42) He never knew the specific reason for his termination, other than there were unspecified "complaints." (Tr. 43) However, he received unemployment, which indicates the termination was not for cause.

At the time of his termination, another systems administrator was terminated, and the project manager left. (Tr. 48, 57) Within a year or so, the company lost the IT support contract and was no longer in the building where Applicant had worked. (Tr. 49)

Policies

When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the adjudicative guidelines. In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially disqualifying conditions and mitigating conditions, which must be considered in evaluating an applicant's eligibility for access to classified information.

These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, these guidelines are applied in conjunction with the factors listed in the adjudicative process. The administrative judge's overarching adjudicative goal is a fair, impartial, and commonsense decision. According to AG ¶ 2(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 interests of 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, the applicant is responsible for presenting "witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by applicant or proven by Department Counsel. . . ." The applicant has the ultimate burden of persuasion to obtain a favorable security decision.

A person who seeks access to classified information enters into a fiduciary relationship with the Government predicated upon trust and confidence. This relationship transcends normal duty hours and endures throughout off-duty hours. The Government reposes a high degree of trust and confidence in individuals to whom it grants access to classified information. Decisions include, by necessity, consideration of the possible risk the applicant may deliberately or inadvertently fail to safeguard classified information. Such decisions entail a certain degree of legally permissible

extrapolation of potential, rather than actual, risk of compromise of classified information.

Section 7 of Executive Order (EO) 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

Adjudicative Guideline (AG) ¶ 39 articulates the security concerns relating to misuse 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, and protection of information.

Applicant was an IT specialist who was terminated from his job in 2006 after 20 years with the company for improperly accessing an internet site. In 2009, he was terminated from his job as an information assurance security officer.

Two of the eight disqualifying conditions under AG ¶ 40 is potentially applicable:

> (e) unauthorized use of a government or other information technology system; and
>
> (g) negligence or lax security habits in handling information technology that persists despite counseling by management.

The only disqualifying condition applicable is AG ¶ 40(e), in that Applicant was not authorized to access the "peer-to-peer" web site. Although he went to the inappropriate site, it appears this occurred through accident, because he did not know the site he was going to was a "peer-to-peer" site. His action was not through negligence or lax security habits. Therefore, AG ¶ 40(g) does not apply. None of the other disqualifying conditions apply. Although he was terminated from employment in July 2009, there does not appear to be any unauthorized use of a government computer, negligence, or lax security habits. None of the disqualifying conditions apply to his July 2009 termination.

Two conditions that could mitigate security concerns that potentially apply are listed in AG ¶ 41 and include:

> (a) so much time has elapsed since the behavior happened, or it happened under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment; 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.

It has been six years since his January-2006 termination. It happened under circumstances that are unlikely to be repeated. Applicant does not go to "peer-to-peer" sites even on his personal computer. The events of January 2006 do not cast doubt on his current reliability, trustworthiness, or good judgment. The second incident involved a new major coming into the work place, making complaints, not telling Applicant what those complaints were, and then having three of the seven individuals at the work location terminated. Applicant received unemployment compensation, which indicates this termination was not for cause. AG ¶ 41(a) applies.

The mitigating factor in AG ¶ 41(c) does not apply. The conduct was unintentional or inadvertent, but there was no prompt, good-faith effort to correct the situation. He made no notification to his supervisor.

Guideline E, Personal Conduct

Adjudicative Guideline (AG) ¶ 15 articulates the security concerns relating 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.

There are two Personal Conduct Disqualifying Conditions under AG ¶ 16, which are potentially applicable:

> (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; and

(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.

The Government argues, under personal conduct, that the two terminations, when considered as a whole, support a whole-person assessment of questionable judgment, trustworthiness, reliability, or an unwillingness to comply with rules and regulations or other characteristics that indicate a person might not safely safeguard protected information. A single event of going to an unauthorized web site six years ago, even though it led to his termination, does not establish a whole-person assessment of questionable judgment or unwillingness to comply with rules.

The record fails to show Applicant did anything wrong resulting in his 2009 termination. Since he received unemployment compensation following that termination, the inference is that it was not a "for cause" termination. It appears, there was a change of command over a very small group of people – seven individuals. After the change of command, there appear to have been some "complaints." The nature, seriousness, Applicant's involvement, or number of complaints are not part of the record. The state of employment being an "at will" state allowed the employer to terminate Applicant and two others, including the site manager. Even with the termination of these individuals, it was a short time before the company was no longer employed on the contract. There is nothing in the record supporting a finding or inference that the second termination was based on questionable judgment, trustworthiness, reliability, or an unwillingness to comply with rules. None of the disqualifying conditions under personal conduct apply to either termination. The case under Guideline E, personal conduct, has not been established.

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 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.

I considered the potentially disqualifying and mitigating conditions in light of all the facts and circumstances surrounding this case. Six years ago, Applicant accessed an inappropriate "peer-to-peer" web site. He was 62 years old, had provided excellent service to the company for more than twenty years, and was being paid more than all but management at the company. Due to this one mistake, which he asserts was an inadvertent error, he was terminated. This single event of going to the inappropriate site may have been an unauthorized use of a government computer, but it was six years ago. The passage of time, without any repeat of the event, mitigates the single act.

Overall, the record evidence leaves me without questions or doubts about Applicant's eligibility and suitability for a security clearance. For all these reasons, I conclude Applicant mitigated the security concerns arising from 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, Information Technology:	FOR APPLICANT
Subparagraphs 1.a and 1.b:	For Applicant
Paragraph 2Personal Conduct:	FOR APPLICANT
Subparagraphs 2.a and 2.b:	For Applicant

Conclusion

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

_____
CLAUDE R. HEINY II
Administrative Judge