DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
----------	)	
SSN: ----------	)	ISCR Case No. 09-01760
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: James F. Duffy, Esquire, Department Counsel
For Applicant: *Pro se*

May 28, 2010

Decision

MALONE, Matthew E., Administrative Judge:

Based upon a review of the pleadings, the Government's exhibits (Gx.), Applicant's exhibits (Ax.), and Applicant's testimony, his request for a security clearance is granted.

On January 2, 2007, Applicant submitted a Questionnaire for Investigation Processing (e-QIP) to renew a security clearance required for his job with a defense contractor. After reviewing the results of the ensuing background investigation, adjudicators for the Defense Office of Hearings and Appeals (DOHA) issued Applicant a set of written interrogatories[1] to clarify or augment information about potentially disqualifying information in his background. After reviewing the results of the background investigation and Applicant's response to the interrogatories, DOHA

[1] Authorized by DoD Directive 5220.6 (Directive), Section E3.1.2.2.

adjudicators were unable to make a preliminary affirmative finding[2] that it is clearly consistent with the national interest to grant Applicant's request for access to classified information. On October 9, 2009, DOHA issued to Applicant a Statement of Reasons (SOR) alleging facts which, if proven, raise security concerns addressed in the adjudicative guidelines (AG)[3] for personal conduct (Guideline E) and misuse of information technology systems (Guideline M).

Applicant timely responded to the SOR and requested a hearing. The case was assigned to me on February 5, 2010. Pursuant to a Notice of Hearing issued the same day, I convened a hearing on February 25, 2010, at which the parties appeared as scheduled. The Government presented five evidentiary exhibits included in the record without objection as Gx. 1 - 5. The Government also proffered two documents for purposes of administrative notice, which were included in the record as Gx. 6 and 7.[4] Applicant testified and presented one witness. The record closed on March 8, 2010, when I received Applicant's post-hearing submission, which has been admitted without objection as Applicant's Exhibit (Ax.) A. DOHA received the transcript of hearing (Tr.) on March 9, 2010.

Findings of Fact

The Government alleged under Guideline M, that, while Applicant was working as an Information Assurance Officer for a defense contractor at a major military installation in February 2008, he intentionally deleted the network account of a person working at that installation. It was further alleged that he did so on two separate occasions and that he was fired for his actions. (SOR 1.a) Under Guideline E, the Government cross-alleged the conduct described in SOR 1.a as adverse personal conduct. (SOR 2.a)

In response to the SOR, Applicant admitted that he deleted the account as alleged, but he denied any malicious intent and denied that he was fired for his conduct. Applicant averred that he resigned his position and accepted employment with another company doing business at the same installation. In addition to the admissions of fact contained in Applicant's answer, I make the following additional findings of relevant fact.

Applicant is 46 years old. He served in the United States Army, primarily in infantry assignments, from November 1982 until he retired as a Sergeant First Class (paygrade E-7) in March 2005. He and his wife have been married since May 1985. They have three children, ages 18, 17, and 10. Applicant has held a security clearance for about 30 years. (Gx. 1)

---

[2] Required by Executive Order 10865, as amended, and by DoD Directive 5220.6 (Directive), as amended.

[3] The adjudicative guidelines were implemented by the Department of Defense on September 1, 2006. Pending official revision of the Directive, they take precedence over the guidelines listed in Enclosure 2 to the Directive.

[4] Identified in the transcript at pp. 15 - 20.

One of Applicant's last active duty assignments in the Army required that he learn the principles of information assurance and information systems security. In November 2004, he completed an Army Information Assurance Security Officer Certification Course. In August 2005, as a civilian, he completed an Army System Administrator Security Course and a Network Manager Security Course. (Tr. 58 - 59; Gx. 5)

After retiring, Applicant went to work for a defense contractor as an Information Security Officer, but left that job in mid-2007 and worked independently doing IT systems installations and other consulting work. In October 2006, he had been appointed as an Information Assurance Security Officer (IASO) by the Army Colonel who was the deputy director of the command where Applicant was working. (Gx. 4) In December 2007, he was hired by another defense contractor at the same Army installation he had worked before as an Information Assurance Officer. He managed, trained, and inspected constituents at that installation. He was also responsible for ensuring his constituents were properly accredited to use their assigned information systems. (Tr. 37 - 38) Accordingly, his duties required that he have privileged access to most aspects of the information systems for which his organization was responsible. Army Regulation (AR) 380-19 governs Information Systems Security throughout the Department of the Army (Gx. 7). Information Assurance at Applicant's job site was governed by a Standard Operating Procedure (SOP) established in November 2006 (Gx. 6). In December 2006, Applicant read and signed a "Network Privileged Access Agreement and Acknowledgment of Responsibilities" form that detailed specific actions, both required and prohibited, for his position. (Gx. 5)

On February 6, 2008, Applicant deleted the unclassified user account of a former co-worker at his previous defense contractor job. Applicant explained that he was "messing around" (Gx. 3) with the system and did not realize he could actually delete someone's account. The person whose account was deleted called the Help Desk and his account was restored. On February 8, 2008, Applicant again deleted the same person's unclassified user account. This time, in response to his Help Desk call, an investigation was conducted that identified Applicant's workstation as the source of the deletion. That same day, Applicant resigned his position in lieu of being fired. (Answer to SOR; Gx. 2)

When Applicant was asked why he had chosen to delete a particular account, he explained that the former co-worker occupied the position that Applicant had held eight months earlier when he worked for that company. That person had been calling Applicant several times each day about what Applicant felt were mundane issues his former co-worker should have been able to resolve on his own. Applicant knew what the job required and could not understand why his former co-worker was bothering him with such questions. Although the first incident was a lark, Applicant admitted that he had become somewhat exasperated and the second incident was more of an attempt to harass the other person. (Tr. 51 - 53) No information, sensitive or otherwise, was lost as a result of Applicant's actions. The information system involved was not compromised in any way by Applicant's actions, but the user affected was unable to access the system for a brief period on the two days in question.

After he resigned, Applicant worked two jobs – at a department store and as a small arms instructor – to support his family. He was hired as an analyst by his current employer, a defense contractor engaged in logistics support for the Army, in September 2008.

Applicant's service in the Army was exemplary. His list of awards and decorations includes a Meritorious Service Medal, three Army Commendation Medals, five Army Achievement Medals, seven Army Good Conduct Medals, a Bronze Star, and a Combat Infantry Badge for deployment to Operation Just Cause in 1989. Applicant completed virtually every infantry training and combat skills course in the Army, served as a Drill Sergeant, and is a graduate of the Advanced Noncommissioned Officer Course. His performance evaluations in the Army were superior, as were his initial civilian on-the-job evaluations. He and his wife have long been active in their church and as volunteers for the House of Heroes, a non-profit organization that helps veterans and public safety personnel, who are disabled, living on a fixed income, or facing other physical or financial challenges, to renovate or repair their homes. These efforts are funded entirely from charitable donations and organized by volunteers such as Applicant and his wife. Applicant enjoys a solid reputation in the community for his integrity, hard work, and reliability. (Ax. A; Tr. 22 - 27)

Policies

Each security clearance decision must be a fair, impartial, and commonsense determination based on examination of all available relevant and material information,[5] and consideration of the pertinent criteria and adjudication policy in the adjudicative guidelines (AG). Decisions must also reflect consideration of the factors listed in ¶ 2(a) of the new guidelines. Commonly referred to as the "whole person" concept, those factors are:

> (1) The nature, extent, and seriousness of the conduct; (2) the circumstances surrounding the conduct, to include knowledgeable participation; (3) the frequency and recency of the conduct; (4) the individual's age and maturity at the time of the conduct; (5) the extent to which participation is voluntary; (6) the presence or absence of rehabilitation and other permanent behavioral changes; (7) the motivation for the conduct; (8) the potential for pressure, coercion, exploitation, or duress; and (9) the likelihood of continuation or recurrence.

The presence or absence of a disqualifying or mitigating condition is not determinative of a conclusion for or against an applicant. However, specific applicable guidelines should be followed whenever a case can be measured against them as they represent policy guidance governing the grant or denial of access to classified information. In this case, the pleadings and the information presented by the parties require consideration of the security concerns and adjudicative factors addressed under

[5] Directive. 6.3.

AG ¶ 15 (Guideline E - Personal Conduct) and AG ¶ 39 (Guideline M - Use of Information Technology Systems).

A security clearance decision is intended to resolve whether it is clearly consistent with the national interest[6] for an applicant to either receive or continue to have access to classified information. The Government bears the initial burden of producing admissible information on which it based the preliminary decision to deny or revoke a security clearance for an applicant. Additionally, the Government must be able to prove controverted facts alleged in the SOR. If the Government meets its burden, it then falls to the applicant to refute, extenuate or mitigate the Government's case. Because no one has a "right" to a security clearance, an applicant bears a heavy burden of persuasion.[7]

A person who has access to classified information enters into a fiduciary relationship with the Government based on trust and confidence. Thus, the Government has a compelling interest in ensuring each applicant possesses the requisite judgment, reliability and trustworthiness of one who will protect the national interests as his or her own. The "clearly consistent with the national interest" standard compels resolution of any reasonable doubt about an applicant's suitability for access in favor of the Government.[8]

Analysis

Use of Information Technology Systems

The Government presented sufficient information to support the allegation in SOR ¶ 1.a. Using his privileged system access as an IASO, Applicant intentionally, but without authorization or other valid reason, deleted a co-worker's user account on an unclassified information of a co-worker if proved, would raise a security concern addressed in AG ¶ 39 as follows:

> 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.

The facts and circumstances of this case require application of the disqualifying condition listed at AG ¶ 40(b) (*illegal or unauthorized modification, destruction,*

[6] *See Department of the Navy v. Egan*, 484 U.S. 518 (1988).

[7] *See Egan,* 484 U.S. at 528, 531.

[8] *See Egan;* Revised Adjudicative Guidelines, ¶ 2(b).

manipulation or denial of access to information, software, firmware, or hardware in an information technology system). Applicant's actions on two occasions in February 2008 clearly denied a co-worker the use of an unclassified system he needed to do his job.

As to AG ¶ 40(a) (*illegal or unauthorized entry into any information technology system or component thereof*), this disqualifying condition does not apply because Applicant's access was legitimate and consistent with his assigned duties. However, AG ¶ 40(e) (*unauthorized use of a government or other information technology system*), applies because he was not authorized to use the system as he did on the occasions at issue.

The disqualifying conditions at AG ¶ 40(c) (*use of any information technology system to gain unauthorized access to another system or to a compartmented area within the same system*); AG ¶ 40(d) (*downloading, storing, or transmitting classified information on or to any unauthorized software, hardware, or information technology system*); AG ¶ 40(g) (*negligence or lax security habits in handling information technology that persist despite counseling by management*), 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*) do not apply based on the facts presented. Finally, AG ¶ 40(h) (*any misuse of information technology, whether deliberate or negligent, that results in damage to the national security*) does not apply because it was not established that any classified information was involved or that the denial of the user's access to his account had any impact on national security.

Applicant has acknowledged the gravity of his conduct, and the record clearly shows that he violated a position of trust, and that he had no valid reason for doing what he did. Accordingly, AG ¶ 41(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*) does not apply. The mitigating condition at AG ¶ 41(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*) does not apply because his conduct was deliberate and he did not act to correct it before he was confronted by his supervisors.

By contrast, the record as a whole supports the mitigating condition at AG ¶ 41(a) (*so much time has elapsed since the behavior happened, or it happened under such unusual circumstances, that it is unlikely to recur or does not cast doubt on the individual's reliability, trustworthiness, or good judgment*). This isolated event occurred more than two years ago. In light of all of the available information about Applicant's military career and his civilian job performance, his conduct in this regard was an aberration. Further, he no longer works as an IASO and is unlikely to seek such a position in the future. On balance, I conclude that available information is sufficient to mitigate the security concerns raised by Applicant's misuse of the information technology system in question.

Personal Conduct

The Government also alleged that Applicant's misuse of technology is disqualifying as adverse personal conduct under Guideline E. (SOR 2.a) This security concern is expressed at AG ¶ 15 as follows:

> 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.

These facts raise the potential applicability of the disqualifying conditions at 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 characteristics indicating that the person may not properly safeguard protected information*); AG ¶ 16(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...(4) evidence of significant misuse of government or other employer's time or resources*); and AG ¶ 16(f) (*violation of a written or recorded commitment made by the individual to the employer as a condition of employment*).

As to AG ¶ 16(f), Applicant signed an agreement to not misuse his position as an IASO with privileged access. He also acknowledged his responsibilities to protect the systems and information to which he had been entrusted. His conduct violated that agreement. As to AG ¶ 16(c), as discussed under Guideline M, above, the information was not sufficient for an adverse determination; however, this disqualifying condition does not apply because of a favorable whole-person analysis, below. Finally, although Applicant misused government resources by deleting a co-worker's account, his conduct is specifically addressed under Guideline M. Accordingly, AG ¶ 16(d) does not apply. The remaining disqualifying conditions under AG ¶ 16 are inapposite to the facts and circumstances of this case.

Available information further requires application of the mitigating condition at AG ¶ 17(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*). For the same reasons discussed under the Guideline M mitigating condition at AG ¶ 41(a), application of AG ¶ 17(c) is sufficient to mitigate the security concerns about Applicant's personal conduct.

Whole-Person Concept

I have evaluated the facts presented and have applied the appropriate adjudicative factors under Guidelines E and M. I have also reviewed the record before me in the context of the whole-person factors listed in AG ¶ 2(a). Applicant is 46 years old, married for 25 years, and the father of three. He is also a distinguished veteran of the U.S. Army, who served for 23 years before retiring in 2005. He has held a security clearance through the military and as a civilian for almost 30 years. His reputation for honesty, hard work, integrity, and reliability is significant. He has acknowledged his wrongdoing in this matter, and he has paid a high professional and personal price for his actions. His resignation in February 2008 resulted in several months of under-employment before he was hired for his current job later that year. Evaluations of his military and civilian job performance have been excellent. All of the information bearing on Applicant's character, judgment, honesty, and reliability indicates that Applicant's continued access to classified information does not present an unacceptable risk to the Government despite the adverse information in his background. A fair and commonsense evaluation of this record shows that the security concerns raised by Applicant's conduct relative to information technology systems and personal conduct are mitigated. Any doubts about Applicant's suitability for access to classified information have been satisfied.

Formal Findings

Formal findings 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:	FOR APPLICANT
Subparagraph 1.a:	For Applicant
Paragraph 2, Guideline E:	FOR APPLICANT
Subparagraph 2.a:	For Applicant

Conclusion

In light of all of the foregoing, it is clearly consistent with the national interest to grant Applicant's request for access to classified information. Request for security clearance is granted.

MATTHEW E. MALONE
Administrative Judge