DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 11-05700
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Caroline H. Jeffreys, Esq., Department Counsel
For Applicant: Gary L. Rigny, Esq.

11/14/2012

Decision

LAZZARO, Henry, Administrative Judge

Applicant is a retired United States Army Colonel who held high-level commands and other responsible positions during his 30 years of military service. He has worked continuously for a defense contractor since he retired from the Army. Applicant possessed a top secret security clearance with sensitive compartmented information (SCI) access for almost 25 years before he committed a security breech due to poor judgment on his part. He mitigated the security concern caused by the mistakes he made over the course of little more than an hour in an otherwise distinguished 36-year career dedicated to national security. Clearance is granted.

On July 25, 2012, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) to Applicant stating it was unable to find it is clearly consistent with the national interest to grant or continue a security clearance for Applicant.[1]

[1] This action was taken under Executive Order 10865, DoD Directive 5220.6, dated January 2, 1992, as amended (Directive), and the adjudicative guidelines which became effective within the Department of Defense for SORs issued after September 1, 2006.

The SOR alleges a security concern under Guideline K (handling protected information). Applicant submitted an undated response to the SOR in which he requested a hearing and admitted the sole SOR allegation.

The case was assigned to me on September 6, 2012. A notice of hearing was issued on September 14, 2012, scheduling the hearing for October 11, 2012. The hearing was conducted as scheduled. The Government submitted four documentary exhibits that were marked as Government Exhibits (GE) 1-4 and admitted into the record without objection. Applicant testified and called two witnesses to testify on his behalf. The transcript was received on October 19, 2012.

Findings of Fact

Applicant's admission to the SOR allegation is incorporated herein. In addition, after a thorough review of the pleadings, testimony, and exhibits, I make the following findings of fact:

Applicant is a 63-year-old man who has been employed as a senior program analyst by a defense contractor since March 2003. He attended college on a Reserve Officers' Training Corps (ROTC) scholarship and was awarded an Army commission in January 1973 following his receipt of a bachelor's degree. Applicant obtained a master's degree in May 1985. He served continuously on active duty in the Army until his retirement at the rank of colonel in January 2003.

Applicant's Army career included the following assignments: assistant program manager for development of an experimental program; command of a battalion; director of a human research and engineering directorate; chief of evaluation for an Assistant Secretary of the Army department; commanding officer of a proving ground; head of the programs and resources division under an Assistant Secretary of the Army; and deputy to a Defense Technology Directorate. Applicant's military awards include three Army Commendation Medals, seven Meritorious Service Medals, and three Legion of Merits.

Applicant has been married since August 1971. He has two adult sons.

Applicant possessed a top secret security clearance with SCI access from 1985 until it was revoked in 2009 due to the incident under consideration herein. Other than that incident, no other action has ever been taken to revoke or downgrade Applicant's security clearance or SCI access based on adverse considerations. No other allegation has ever been made indicating Applicant ever mishandled or risked the compromise of classified information.

In April 2009, Applicant drafted an unclassified power-point presentation that was to be presented by a program manager located in another state. Applicant was instructed to modify the presentation by including classified information to limit the people who would be able to attend the presentation. Applicant, with the assistance of two other people,

inserted information in the power-point presentation that made it a classified document which was then saved on a classified computer.

On April 15, 2009, Applicant received a request on behalf of the program manager who was to make the presentation to have an unclassified version of the presentation transmitted to her. Applicant was alone in his work space when the request was received and he decided he would declassify the presentation by himself and submit it as requested. Due to the physical limitations of the work space, Applicant was unable to print out the presentation and sterilize it from a hard copy. He therefore concluded he would sterilize the presentation on a classified computer, download the sterilized presentation onto a disc, and transmit it by e-mail.

Applicant thereafter inserted an unclassified disc into the classified computer, downloaded what he believed was a sanitized version of the presentation onto the unclassified disc, and transmitted it to the person who had requested it via an e-mail sent over an unclassified network. The recipient immediately recognized the presentation contained material that made it a classified document and so notified Applicant. The level of classification is not of record herein.

Applicant placed the disc which contained the material into a safe. Although the disc should have been marked indicating it contained classified information, Applicant did not do so. The disc remained in the safe overnight. Applicant notified his employer's facility security officer and his supervisor, the company's executive vice president, of the incident at 7:39 AM on April 16, 2009. Immediate action was then taken to prevent any further possibility of dissemination of the material.

Applicant acknowledges the serious errors in judgment he committed on April 15, 2009. Those include downloading material onto a disc from a classified computer without marking the disc as classified, attempting to sterilize a classified program without his work being checked by a second person, and transmitting classified information over an unclassified network.

Applicant has taken action to prevent any future reoccurrence by successfully completing between five and seven courses on computer security and handling classified information. Applicant's employer was informed of the security breech and, although Applicant was no longer able to work on the program to which he had been assigned, elected to retain Applicant in a position in which he does not have access to classified information.

Policies

The Directive sets forth adjudicative guidelines to consider when evaluating a person's eligibility to hold a security clearance. Chief among them are the disqualifying and mitigating conditions for each applicable guideline. Each clearance decision must be a fair and impartial decision based upon relevant and material facts and circumstances, the

whole-person concept, and the factors listed in ¶ 6.3.1 through ¶ 6.3.6 of the Directive. Although the presence or absence of a particular condition or factor for or against clearance is not outcome determinative, the adjudicative guidelines should be followed whenever a case can be measured against this policy guidance. Guideline K (handling protected information) with its disqualifying and mitigating conditions, is most relevant in this case.

The sole purpose of a security clearance decision is to decide if it is clearly consistent with the national interest to grant or continue a security clearance for an applicant.[2] The Government has the burden of proving controverted facts.[3] The burden of proof in a security clearance case is something less than a preponderance of evidence,[4] although the Government is required to present substantial evidence to meet its burden of proof.[5] "Substantial evidence is more than a scintilla, but less than a preponderance of the evidence."[6] Once the Government has met its burden, the burden shifts to an applicant to present evidence of refutation, extenuation, or mitigation to overcome the case against him.[7] Additionally, an applicant has the ultimate burden of persuasion to obtain a favorable clearance decision.[8]

No one has a right to a security clearance[9] and "the clearly consistent standard indicates that security clearance determinations should err, if they must, on the side of denials."[10] Any reasonable doubt about whether an applicant should be allowed access to classified information must be resolved in favor of protecting national security.[11]

Analysis

Paragraph 33 of the adjudicative guidelines sets out the security concern relating to handling protected information:

---

[2] ISCR Case No. 96-0277 (July 11, 1997) at 2.

[3] ISCR Case No. 97-0016 (December 31, 1997) at 3; Directive, Enclosure 3, Item E3.1.14.

[4] *Department of the Navy v. Egan* 484 U.S. 518, 531 (1988).

[5] ISCR Case No. 01-20700 (December 19, 2002) at 3 (citations omitted).

[6] ISCR Case No. 98-0761 (December 27, 1999) at 2.

[7] ISCR Case No. 94-1075 (August 10, 1995) at 3-4; Directive, Enclosure 3, Item E3.1.15.

[8] ISCR Case No. 93-1390 (January 27, 1995) at 7-8; Directive, Enclosure 3, Item E3.1.15.

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

[10] *Id.* at 531.

[11] *Egan*, Executive Order 10865, and the Directive.

> Deliberate or negligent failure to comply with rules and regulations for protecting classified or other sensitive information raises doubt about an individual's trustworthiness, judgment, reliability, or willingness and ability to safeguard such information and is a serious security concern.

On April 15, 2009, Applicant improperly downloaded classified information from a classified computer onto a disc that was not marked as containing classified information. He attempted to declassify a power-point presentation by himself without having his work checked by a second person, contrary to proper security protocol. He then transmitted classified information via an unclassified network. Disqualifying Conditions (DC) 34(a): *deliberate or negligent disclosure of classified or other protected information to unauthorized persons . . .* ; DC 34(c): *loading, drafting, editing, modifying, storing, transmitting, or otherwise handling classified reports, data, or other information on any unapproved equipment including but not limited to any typewriter, work processor, or computer hardware, software, drive, system, gameboard, handheld, "palm" or pocket device or other adjunct equipment;* and DC 34(g): *any failure to comply with rules for the protection of classified or other sensitive information* apply.

Applicant had a stellar 30-year military career during which he held a top secret security clearance and SCI access without incident. He worked for his defense contractor employer while possessing a top secret security clearance and SCI access for six years before the security concerns at issue herein occurred. This incident occurred when Applicant attempted to comply with a request from a program manager for immediate provision of information under an unusual circumstance where Applicant found himself alone in his work space. He took immediate and appropriate action to alleviate the potential harm that might have occurred from his improper downloading, storing, and transmitting classified information. Applicant has successfully completed remedial training in computer security and handling classified information in an effort to make certain his one-time lapse of judgment does not recur.

The following Mitigating Conditions (MC) apply: MC 35(a): *so much time has elapsed since the behavior, or it has happened so infrequently or under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or good judgment*; and MC 35(b): *the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities.*

Applicant receives substantial credit under a whole-person analysis for his distinguished military career, which included high-level commands and other demanding and responsible positions. He is credited with the many years he held a top secret security clearance and SCI access without incident. Applicant's 41-year marriage and continuous employment by a single defense contractor since his military retirement are indicative of a secure and stable lifestyle. Applicant displayed integrity by promptly self-reporting his error and acknowledging his mistakes. He has taken aggressive action by completing a

number of remedial security awareness programs to make himself a person who can once again be trusted to possess and protect classified information.

Considering all relevant and material facts and circumstances present in this case, the factors listed in ¶ 6.3.1 through ¶ 6.3.6 of the Directive, the whole-person concept, and the applicable disqualifying and mitigating conditions, I find Applicant mitigated the handling protected information security concern. Applicant has overcome the case against him and satisfied his ultimate burden of persuasion. It is clearly consistent with the national interest to grant Applicant a security clearance. Guideline K is decided for Applicant.

Formal Findings

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

Paragraph 1, Guideline K:	FOR APPLICANT
Subparagraph 1.a:	For Applicant

Conclusion

In light of all the circumstances presented by the record in this case, it is clearly consistent with the national interest to grant or continue a security clearance for Applicant. Clearance is granted.

_____
Henry Lazzaro
Administrative Judge