DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
----------	)	ISCR Case No. 07-04847
SSN: ----------	)	
	)	
Applicant for Security Clearance	)	

Appearances

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

June 30, 2008

Decision

FOREMAN, LeRoy F., Administrative Judge:

This case involves security concerns raised under Guidelines K (Handling Protected Information) and E (Personal Conduct). Applicant mitigated the security concerns under Guideline K, but not under Guideline E. Eligibility for access to classified information is denied.

Statement of the Case

Applicant submitted his Security Clearance Application (SF 86) on November 18, 2002. On August 20, 2007, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) detailing the basis for its preliminary decision to deny his application, citing security concerns under Guidelines K and 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 revised adjudicative guidelines (AG) promulgated by the President on December 29, 2005, and effective within the Department of Defense for SORs issued after September 1, 2006.

Applicant acknowledged receipt of the SOR on August 27, 2007; answered it on September 14, 2007; and requested a hearing before an administrative judge. DOHA received the request on September 19, 2007. Department Counsel was prepared to proceed on December 31, 2007, and the case was assigned to me on January 2, 2008. The case was tentatively scheduled for February 29, 2008. Applicant retained a lawyer, who entered his appearance on January 29, 2008, and requested that the hearing be postponed until March 2008. His entry of appearance and request for a postponement are attached to the record as Hearing Exhibit (HX I).

DOHA issued a notice of hearing on March 27, 2008, scheduling the hearing for April 24, 2008. I convened the hearing as scheduled. Government Exhibits (GX) 1 through 28 were admitted in evidence without objection. The testimony of one government witness was taken by video-teleconference (VTC), and two government witnesses testified in person at the hearing. Department Counsel's request to present the testimony of one witness by VTC is attached to the record as HX II. Applicant testified on his own behalf, and submitted Applicant's Exhibits (AX) A through Z, which were admitted without objection.

I granted Applicant's request to keep the record open until May 9, 2008, to enable him to submit additional documentary evidence. Applicant timely submitted AX AA through DD, and they were admitted without objection. I granted requests from counsel for both sides to submit written closing statements. Department Counsel's written closing statement is attached to the record as HX III, and Applicant's counsel's closing statement is HX IV. The record closed on May 9, 2008. DOHA received the transcripts of the VTC testimony and the hearing (Tr.) on May 15, 2008. The VTC testimony is in a separate transcript marked "VTC Transcript."

Findings of Fact

In his answer to the SOR, Applicant denied all the allegations. At the hearing, he admitted the facts alleged in SOR ¶¶ 1.a and 1.b, and his admissions are incorporated in my findings of fact. I make the following findings:

Applicant is a 63-year-old mechanical engineer. He has held a security clearance since August 1967. He received a Ph.D. in mechanical engineering in 1980 and worked for a defense contractor until December 1998. He formed his own company in February 1999 and works as a consultant to defense contractors in the field of underwater acoustics (Tr. 166). He is the president and sole owner of his company. He also is the Information System Security Manager (ISSM) and the Facility Security Officer (FSO). His daughter is the corporate secretary and his brother is the chairman of the board (Tr. 174).

Applicant requested a facility security clearance in October 1999, and his company was granted a clearance in September 2000. The cognizant security agency (CSA) for Applicant's company is the Defense Security Service (DSS), as executive

agent for the Department of Defense (Tr. 47). A DSS industrial security representative (ISR) conducted a security inspection of the facility in December 2000, and Applicant received an updated copy of Chapter 8 of the National Industrial Security Program Operating Manual (NISPOM) from DSS in February 2001 (AX W). The ISR acts for DSS in interpreting the NISPOM (Tr. 47).

Applicant's ISR testified he and Applicant had an open, cooperative, and cordial relationship (Tr. 73). He testified that establishing an information system (IS) for the first time in a small organization can be "fairly daunting," but Applicant was receptive to advice (Tr. 76). The ISR had complained to his supervisors on "more than one occasion" about the difficulty of monitoring a company where the president, owner, facility security officer, and information security manager were the same person (Tr. 113).

The ISR normally corresponds by email. He works a normal 5-day week, and his workday ends at 4:30. His Blackberry shuts off at 4:30. He responds to emails received after 4:30 during the next duty day (Tr. 101-02).

Applicant's company received interim accreditation for processing classified information in September 2001 (AX L). After a number of discussions with his ISR and several modifications of his company's draft Information System Security Plan (ISSP), his ISSP dated December 4, 2001, was approved and fully accredited by DSS on January 17, 2002 (GX 7; GX 21; AX M; Tr. 172). Although Applicant held a clearance for many years, this was his first experience developing an ISSP (Tr. 172).

The ISSP recites that it was written in accordance with the NISPOM, Industrial Security Letter (ISL) 00L-2, and ISL 01L-1 (GX 7 at ¶ 1.1). ISL 01L requires that DSS be notified before any changes to an ISSP are implemented so a reaccreditation decision can be made. It also requires that classified processing be in an area where authorized contractor personnel can exercise constant surveillance and control. It must have an "an identifiable boundary (e.g., walls, signs, tape on floor, rope or chains) where it is obvious that the area is restricted to only authorized personnel." The "identifiable boundary" for Applicant's information system (IS) was the living room of his home, where he lives alone (Tr. 43).

The ISSP designated Applicant as the ISSM and stated: "Management assures that the ISSM is trained to a level commensurate with the complexity of the facility's [information system]. In this role, the ISSM shall carry out all duties as outlined in Section 8, 103 of the NISPOM." (GX 7 at ¶ 2.2.) The NISPOM ¶ 8-103b states that the ISSM "[e]stablishes, documents, implements, and monitors the IS Security Program and related procedures for the facility and ensures facility compliance with requirements for IS." The letter from DSS approving the ISSP reminded Applicant of his responsibility as ISSM "to ensure that any change in configuration, mode of operation or other modification is analyzed to determine its impact and to take appropriate action, including notification of this office, in order to maintain a level of security consistent with the requirements for this accreditation."

The ISSP "Hardware Baseline" listed one laptop computer, a monitor, two printers, and two disk drives (GX 8, Attachment 3). Applicant used the laptop for both classified and unclassified processing by switching removable hard drives (Tr. 177).

On November 20, 2002, Applicant completed an on-line course of instruction from the DSS Academy entitled "Essentials of Industrial Security Management" (AX A). On December 1, 2002, he completed an on-line DSS course entitled "Protecting Secret and Confidential Documents" (AX B). He enrolled in a resident DSS course entitled "FSO Program Management" in February 2003 but did not attend the course because it conflicted with a scheduled briefing for a project (AX D; Tr. 175). He completed the "FSO Program Management" course in July 2003.

On Sunday, February 16, 2003, Applicant traveled across the country from his home to give a four-hour classified presentation to a defense contractor. He had prepared the presentation in his home office, the designated site in his ISSP (Tr. 180). The host contractor had agreed to provide a classified computer for the presentation (Tr. 181). However, on the evening of Friday, February 14, 2003, Applicant was informed by the host contractor's security representative that he had been unable to obtain a computer for the presentation, and Applicant offered to use his computer in a classified mode if they could not find a suitable computer at the site of the presentation (Tr. 182).

Applicant traveled to the site of the presentation with his laptop computer, a classified hard drive, and a compact disc classified SECRET. He arrived late at night and stored the classified hard drive and classified compact disc in a safe at the host contractor's security office (AX BB). He kept his laptop in his possession, because there was insufficient space for it in the safe. He testified he did not think it was necessary to store the laptop in the safe because the classified hard drive had been removed and his laptop had several security seals on it (GX 12 at 3-4).

Applicant testified he believed the restrictions on removal of hardware in the ISSP applied only to doing classified processing outside his approved work space in his office (Tr. 183). He had taken his computer off-site on other occasions, but only with the shell of the computer and the unclassified hard drive. He would follow the downgrade procedure in his ISSP, remove the classified drive, and record the downgrade in a log (Tr. 185). The trip in February 2003 was the first time he had taken his laptop off-site to do classified work. He testified he did not contact his ISR for permission because he did not think it was necessary (Tr. 186). He also testified he did not contact his ISR for permission to bring classified material to the host-contractor's site because he did not think it was required (Tr. 188). In his capacity as FSO, he signed the courier letter authorizing him to hand-carry the classified material to the host contractor's site (AX AA).

On Monday, February 17, 2003, after arriving at the host contractor's site, he revised Attachment 2 to his ISSP, entitled "System Identification and Requirements

Specification, by adding the following sentence: "This IS contains a portable Laptop PC used in the Standalone mode for classified presentations and the processing of classified acoustic data at [Applicant's company name] customer facilities capable of handling classified information up to the level of secret." He revised Attachment 3, entitled "Hardware Baseline" to add a Sony memory stick. He saved the revisions on his laptop but did not print them. He testified he thought it was likely he would need to use his computer in a classified mode on the following day, and he used his free time on the evening of February 17 to make the changes to his ISSP. He did not consult with or notify his ISR about the changes. He denied making the changes in anticipation of someone at the host contractor's site confronting him about his authority to do classified work on his computer at that location (Tr. 274-75).

Because of inclement weather, the arrival of the attendees for the presentation was delayed and the time allotted for his presentation was cut from four hours to two (Tr. 192-93).

On February 18, 2003, Applicant purchased the memory stick listed on Attachment 3 and copied his classified presentation onto it (GX 12 at 2; Tr. 198). He used his own laptop for classified work because the host contractor had been unable to timely provide him with a classified computer at its facility (Tr. 194). He did not notify his ISR that the memory stick had been added to his information system.

On February 19, 2003, Applicant provided the Sony memory stick to a host contractor employee for use in a host contractor computer during his classified presentation. After his presentation, he mailed the Sony memory stick, classified hard drive, and classified compact disc back to his office. He hand-carried his laptop, without the classified hard drive, authorized by a courier letter he had signed as FSO (AX AA).

On February 26, 2003, Applicant returned to the host contractor's site. He hand-carried the Sony memory stick containing his classified presentation and a classified compact disc. He used his memory stick in a host contractor's computer for his presentation, and then hand-carried both the memory stick and classified compact disc back home on a commercial aircraft. Again, he signed the courier letter as FSO (AX CC).

Applicant testified he did not believe the addition of the memory stick to his ISSP required reaccreditation, because it was removable media, like a CD or DVD. He has since learned that it is considered a hard drive and requires reaccreditation (Tr. 267).

The ISR overseeing Applicant's company since 2001 testified that accreditation is a government function, but that certification can be done by a contractor if DSS authorizes self-certification. Authority to self-certify must be requested as part of the ISSP, and DSS would determine whether the contractor has the technical experience and skills to convince DSS to allow self-certification (Tr. 30-32). The ISR testified that Applicant did not have authority to self-certify (Tr. 33, 69-70).

The ISR testified that Applicant's relocation of his laptop computer and the addition of the memory stick were two changes requiring notification of the CSA and reaccreditation under NISPOM ¶ 8-104f (Tr. 50-51). This provision requires notification of the CSA "when an IS no longer processes classified information, or when changes occur that might affect accreditation." NISPOM ¶ 8-202c provides, "All modifications to security-relevant resources (including software, firmware, hardware, or interfaces and interconnections to networks) shall be reviewed and approved in accordance with procedures prior to implementation." ISL 01L-1, cited in Applicant's ISSP, defines "security-relevant" hardware changes requiring review and approval as "any IS component that contains, or has the potential of containing classified information." The ISR testified that if Applicant was unsure whether addition of the memory stick was a "security relevant" change, he was expected to contact his ISR for a ruling before he implemented it (Tr. 51).

The ISR further testified that even the "shell" of a laptop, with the hard drive removed, is required to be kept within the perimeter of the site documented in the ISSP. If Applicant wanted to remove his laptop, even without the classified hard drive, he was required to notify DSS and obtain approval to remove it. If he later returned the laptop to the designated site, he was required to request reactivation of the prior approval, and DSS would determine whether an on-site inspection was required prior to reactivation (Tr. 55). The NISPOM ¶ 8-308a requires establishment of safeguards to detect "unauthorized modification of the IS hardware and software." It further provides that "[h]ardware integrity of the IS, including remote equipment, shall be maintained at all times, even when all classified information has been removed from the IS." The NISPOM ¶ 8-308b provides that "Classified information shall take place in a CSA-approved area." Applicant did not dispute any of the ISR's interpretations of the NISPOM or ISL 01L-1.

While Applicant was editing his classified presentation on his laptop on February 18, 2003, he was asked by the host contractor's FSO if he was authorized to process classified material outside his own facility. The evidence regarding his response is conflicting.

During the ISR's inquiry into the report of Applicant's security violations in March 2003, the FSO said she asked Applicant about his usage of his laptop to process classified information at their facility. She wanted to know if he had "signed DSS approval for his AIS plan allowing usage of that laptop at other facilities for classified processing." She stated Applicant responded, "Yes, I do have approval from my DSS rep to use this company laptop at other facilities to process classified." He also told her he had used his laptop to process classified material at other facilities. She asked Applicant to provide her with a copy of the DSS approval and he agreed (GX 20 at 14). Applicant admitted to the ISR that he said he had DSS approval even though approval had not been requested and he admitted misleading the FSO by telling her he had used his laptop to process classified material at other facilities because he wanted her to go away and stop interfering with his work. Applicant told the ISR that he had never processed classified materials on his laptop at other facilities (GX 20 at 5-6).

When the ISR interviewed Applicant, he was not sure Applicant knew he had committed a security violation (Tr. 93). However, the ISR came to the conclusion that Applicant's violations were willful and knowing because he created the false document purporting to change the ISSP (Tr. 87). The ISR testified the document was false because Applicant represented it as having been approved by DSS, when it was not (Tr. 90). The ISR concluded there was no unauthorized disclosure of classified information (Tr. 109).

In a statement to a security investigator in November 2003, Applicant stated the host contractor's FSO wanted to see a copy of the DSS approval to process classified material on his laptop at their site, and he agreed to send it to her. Applicant told the investigator he did not remember saying he had used his laptop for classified work at other facilities. He admitted being unresponsive to her questions because she was interfering with his work (GX 12 at 2).

In an interview with another security investigator in April 2004, he admitted trying to mislead the host contractor's FSO (VTC Tr. 11-12; GX 18). He admitted telling her he had DSS approval to use his laptop at other facilities and had done so in the past (GX 18 at 2).

In November 2005, another government agency notified Applicant of its intent to revoke his eligibility for access to sensitive compartmented information (SCI). One of the allegations on which the intent to revoke was based was his admission that he intentionally misled the host contractor's FSO by stating he had DSS approval to use his laptop at other facilities and had done so in the past. He responded to the notice of intent to revoke by stating, "This allegation is true, but there is an explanation." He then described the host contractor's failure to provide a classified computer, the need to revise the presentation on short notice, and his frustration and impatience when the FSO challenged him (GX 25 at 5).

At the hearing, Applicant recanted his earlier admissions to intentionally misleading the host contractor's FSO (Tr. 285). He testified the FSO asked if he was working on a classified information system and he told her he had DSS approval to use his laptop as a classified information system (Tr. 201). He testified he told her he was the ISSM and he had revised his ISSP to authorize working with classified information on his laptop at other facilities (Tr. 203). He testified he was confused about what she was asking for, because she was concerned about two issues—his authority to use his laptop for classified work and his authority to use his laptop at the host contractor's site. He testified he did not intentionally mislead the host contractor's FSO, and that he did not tell her he had DSS approval for off-site classified work on his laptop because he knew he did not have it (Tr. 214). He testified he did not intend to mislead her, but that his intention was "just to go back to work." He believed he was answering different questions than she was asking and he did not understand what she was asking (Tr. 291). He did not believe he told her he had used his laptop to process classified

information off-site on other occasions (Tr. 216). He testified the conversation was "curt," and "not particularly" cordial (Tr. 215).

At some time after February 18, 2003, the host contractor notified its local ISR about Applicant's use of his laptop for classified work, and the local ISR notified Applicant's ISR on March 10, 2003. The ISR conducted the administrative inquiry discussed above, and he concluded that Applicant knowingly and intentionally violated various provisions of the NISPOM, prepared a falsified ISSP, and falsely represented to the host contractor that the revised ISSP was approved by DSS. The ISR recommended the accreditation for Applicant's ISSP be withdrawn, but his recommendation was not adopted. Applicant's ISSP was reaccredited in November 2004 (AX O) and June 2005 (AX Q).

As a result of the administrative inquiry, the chairman of the board of Applicant's company required him to execute a "letter of commitment" to full compliance with all applicable security measures, write a supplement to the security regulations applicable to the company, provide the chairman with copies of documentation pertaining to the processing, storage, and handling of classified information, and to pay a fine of one week's pay, about $1,600. The money was donated to a high school scholarship fund in memory of a U.S. Marine killed in Iraq (Tr. 227; GX 14 at 3; AX Y; AX Z). Applicant testified he intends to transfer ownership of the company to his brother, the current chairman of the board, as part of the mitigation plan to retain his facility clearance (Tr. 235).

In May 2003, Applicant submitted a revised ISSP adding the Sony memory stick to his information system (GX 10, Attachment 8). He had submitted a revised ISSP with the authorization for off-site classified work on his laptop, but he removed that provision in accordance with his ISR's guidance (Tr. 223).

In an interview with a DSS agent in April 2004, Applicant admitted he used the same laptop for classified and unclassified work and that he took the laptop with him for almost all trips, as well as trips to his son's house, daughter's house, and his leased office space, a total of about 24 times until February 2003 (GX 15). At the hearing, he testified he believed it was permissible to remove the laptop from his designated work space without violating any rules, so long as he removed and secured the classified hard drive. When advised that it was a security violation to remove the laptop from his cleared facility, even if the classified drive was removed, he purchased a second laptop for unclassified work away from his cleared facility (Tr. 224).

The NISPOM ¶ 1-201 requires that an FSO complete the security training specified in the NISPOM and "as deemed appropriate by the CSA." At the hearing, Applicant admitted it was a mistake to delay his training as an FSO. He testified that what he learned in the FSO management course could have prevented "almost all of this stuff" from happening. He testified he cannot afford to make the same mistakes again. He has learned that there are requirements in the NISPOM that are unclear, and that he should discuss all changes with his ISR to avoid further mistakes (Tr. 236).

On March 28, 2008, Applicant's personal security clearance was suspended because of a decision by another government agency to revoke his eligibility for access to (SCI) (AX T). The basis for the revocation of SCI access included the conduct alleged in the SOR (AX U). According to his ISR, Applicant was completely cooperative when the ISR came to his home office to clear out his safe (Tr. 85).

Policies

"[N]o one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988). As Commander in Chief, the President has the authority to control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to have access to such information." *Id.* at 527. The President has authorized the Secretary of Defense or his designee to grant applicants eligibility for access to classified information "only upon a finding that it is clearly consistent with the national interest to do so." Exec. Or. 10865, *Safeguarding Classified Information within Industry* § 2 (Feb. 20, 1960), as amended and modified.

Eligibility for a security clearance is predicated upon the applicant meeting the criteria contained in the revised adjudicative guidelines (AG). These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, these guidelines are applied in conjunction with an evaluation of the whole person. An administrative judge's over-arching adjudicative goal is a fair, impartial and common sense decision. An administrative judge must consider all available, reliable information about the person, past and present, favorable and unfavorable.

The government reposes a high degree of trust and confidence in persons with access to classified information. This relationship transcends normal duty hours and endures throughout off-duty hours. Decisions include, by necessity, consideration of the possible risk the 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.

Clearance decisions must be "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." *See* Exec. Or. 10865 § 7. Thus, a decision to deny a security clearance is not necessarily a determination as to the loyalty of the applicant. It is merely an indication the applicant has not met the strict guidelines the President and the Secretary of Defense have established for issuing a clearance

Initially, the government must establish, by substantial evidence, conditions in the personal or professional history of the applicant that may disqualify the applicant from being eligible for access to classified information. The government has the burden of establishing controverted facts alleged in the SOR. *See Egan*, 484 U.S. at 531. "Substantial evidence" is "more than a scintilla but less than a preponderance." *See v.*

Washington Metro. Area Transit Auth., 36 F.3d 375, 380 (4th Cir. 1994). The guidelines presume a nexus or rational connection between proven conduct under any of the criteria listed therein and an applicant's security suitability. *See* ISCR Case No. 95-0611 at 2 (App. Bd. May 2, 1996).

Once the government establishes a disqualifying condition by substantial evidence, the burden shifts to the applicant to rebut, explain, extenuate, or mitigate the facts. Directive ¶ E3.1.15. An applicant "has the ultimate burden of demonstrating that it is clearly consistent with the national interest to grant or continue his security clearance." ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002). "[S]ecurity clearance determinations should err, if they must, on the side of denials." *Egan*, 484 U.S. at 531; *see* AG ¶ 2(b).

Analysis

Guideline K, Handling Protected Information

The SOR alleges Applicant willfully and deliberately violated the NISPOM by accessing classified information on his DSS accredited laptop at a host contractor's facility without prior DSS authorization or approval (SOR ¶ 1.a); he willfully and deliberately violated the NISPOM by bringing a classified hard drive to a host contractor's facility and downloading classified material onto a memory stick (SOR ¶ 1.b); and he deliberately violated the NISPOM by altering classified material by obliterating the classified markings on 10 pages of a 50-page document without notifying his security manager (SOR ¶ 1.c). Department Counsel elected not to present evidence or otherwise pursue SOR ¶ 1.c (Tr. 4).

The security concern relating to Guideline K is set out in AG ¶ 33 as follows: "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."

The following potentially disqualifying conditions under this guideline are relevant to this case:

> Collecting or storing classified or other protected information at home or in any other unauthorized location (AG ¶ 34(b));
>
> 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, word processor, or computer hardware, software, drive, system, gameboard, handheld, "palm" or pocket device or other adjunct equipment (AG ¶ 34(c)); and

Any failure to comply with rules for the protection of classified or other sensitive information (AG ¶ 34(g)).

Applicant's removal of his laptop from its approved location, use of the laptop at an unapproved location, and use of an unapproved memory stick raise AG ¶¶ 34(b), (c), and (g). Since the government produced substantial evidence to raise these disqualifying conditions, the burden shifted to Applicant to produce evidence to rebut, explain, extenuate, or mitigate the facts. Directive ¶ E3.1.15. An applicant has the burden of proving a mitigating condition, and the burden of disproving it never shifts to the government. *See* ISCR Case No. 02-31154 at 5 (App. Bd. Sep. 22, 2005).

Security concerns under this guideline can be mitigated by showing "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" (AG ¶ 35(a).) This condition has three disjunctive prongs and one conjunctive prong. It can be established if "so much time has elapsed," or it happened "so infrequently" or "under such unusual circumstances" that it is unlikely to recur. If any of the three conjunctive prongs are established, the mitigating condition is not fully established unless the behavior "does not cast doubt" on reliability, trustworthiness, or good judgment. The first prong is established because Applicant's behavior happened more than five years ago and has not recurred. The second prong is established because the violations occurred on only two occasions in February 2003. These were his only security violations during the 40-year period in which he held a clearance. The third prong is established because the violations were the result of a confluence of unusual conditions that are not likely to recur: Applicant's inadequate training for his responsibilities as ISSM and FSO, delay of the briefing by bad weather, a requirement to drastically edit the briefing when the allotted time was cut in half, and inability of the host contractor to provide a classified computer for the editing process.

The last prong, however, is not established because Applicant's deceptive responses to the host contractor's FSO, representation that DSS had approved his modified ISSP allowing off-site use of his laptop for classified work, and his recantation at the hearing of his prior admissions cast doubt on his current reliability, trustworthiness, and good judgment. The inconsistency between Applicant's multiple admissions to intentionally misleading the FSO and his recantation of those admissions at the hearing means that either his earlier admissions or his recantation at the hearing were untrue. Either alternative would raise doubt about his reliability and trustworthiness.

I found Applicant's recantation of his earlier admissions at the hearing not credible. He consistently admitted intentionally misleading the FSO during the inquiry by his ISR in March 2003, during an interview with a security investigator in April 2004, during an interview with another security investigator in April 2004, and in his response to the notification of intent to revoke his eligibility for access to SCI in November 2005. The evidence strongly suggests his recantation at the hearing was prompted by the

revocation of his SCI eligibility and the realization that his security clearance and ability to continue working as a consultant were in jeopardy.

Applicant's recantation was not alleged in the SOR, however, conduct not alleged in the SOR may be considered: "(a) to assess an applicant's credibility; (b) to evaluate an applicant's evidence of extenuation, mitigation, or changed circumstances; (c) to consider whether an applicant has demonstrated successful rehabilitation; (d) to decide whether a particular provision of the Adjudicative Guidelines is applicable; or (e) to provide evidence for whole person analysis under Directive Section 6.3." ISCR Case No. 03-20327 at 4 (App. Bd. Oct. 26, 2006) (citations omitted). I considered his recantation for the limited purposes of accessing his credibility, to decide whether the conduct alleged in the SOR casts doubt on his current reliability, trustworthiness, or good judgment, and in my whole-person analysis set out below.

Security concerns also can be mitigated by evidence that "the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities." (AG ¶ 35(b).) I am satisfied Applicant's unauthorized use of his laptop for classified work at the host contractor's site and his unauthorized use of the memory stick were inadvertent violations. He volunteered the use of his computer when it appeared that a classified computer would not be available at the contractor's site. Because of his limited experience and lack of training as an ISSM and FSO, he believed he had authority to modify his ISSM. It was not until he was challenged by the contractor's FSO that he realized he might need his DSS approval for remote use of his laptop for classified work. I found his explanation for using the memory stick, i.e., that he thought it was removable media that did not require DSS approval, was plausible and credible. He finally completed his FSO training, obtained DSS approval for his modified ISSP, acquired a second computer dedicated to unclassified work, and has had no further security violations. I conclude AG ¶ 35(b) is established.

Finally, security concerns under this guideline can be mitigated by showing that "the security violations were due to improper or inadequate training." (AG ¶ 35(c).) At the time of the violations, Applicant had completed online courses regarding the handling of classified information, and he appears to have complied fully with the NISPOM when he transported and secured his classified materials in February 2003. Although his ISSP was approved and accredited in December 2001, he still had not completed his FSO training when the violations occurred in February 2003. He admitted at the hearing that the violations would not have occurred if he had timely completed the FSO hearing. However, while the inadequate training caused the violations, the fault lies with Applicant for not timely completing it. Applicant receives only limited mitigation under AG ¶ 35(c) because his culpable failure to attend FSO training was a major factor in causing the violations.

Guideline E, Personal Conduct

The SOR cross-alleges the SOR ¶¶ 1.a, 1.b, and 1.c as personal conduct under this guideline (SOR ¶ 2.a). It also alleges Applicant deliberately attempted to cover up his security violations by falsely stating he had DSS authority to use his laptop at other facilities (SOR ¶ 2.b) and by revising his ISSP to authorize using his laptop to process classified information at other facilities (SOR ¶ 2.c).

The security concern under this guideline is set out in 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." A potentially disqualifying condition under this guideline can be raised by "deliberately providing false or misleading information concerning relevant facts to an employer, investigator, security official, competent medical authority, or other official government representative" (AG ¶ 16(b).) Applicant's false and misleading responses to the host contractor's FSO and his representation that he had DSS approval for remote use of his laptop for classified work raise this condition.

A potentially disqualifying condition also may arise from "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(c).) While Applicant presented substantial mitigating evidence regarding his security violations under Guideline K, his misrepresentations to the contractor's FSO and his lack of candor at the hearing are sufficient to raise this disqualifying condition under Guideline E.

Finally, a potentially disqualifying condition may arise from "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." (AG ¶ 16(d).) This disqualifying condition encompasses "untrustworthy or unreliable behavior" and "a pattern of dishonesty or rule violations." (AG ¶¶ 16(1) and (3).)

On its face, AG ¶ 16(d) appears to cover only information "that is not explicitly covered under any other guideline." The Appeal Board, however, has construed AG ¶ 16(d) more broadly, holding: "(1) it continues the longstanding tenet that specific behavior can have security significance under more than one guideline and (2) by focusing on the concepts of questionable judgment and irresponsibility, it contemplates that behavior will have independent security significance under Guideline E in a broad

range of cases." ISCR Case No. 06-20964 (App. Bd. Apr. 10, 2008), 2008 WL 2002589 at *4. I conclude AG ¶ 16(d) is raised by Applicant's misleading responses to the FSO and his false representation that DSS had approved his modified ISSP.

Security concerns under this guideline can be mitigated by showing "the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts." AG ¶ 17(a). Applicant made no effort to correct his misrepresentations to the FSO until the host contractor's ISR contacted Applicant's ISR, who questioned him about the incident. I conclude this mitigating condition is not established.

Security concerns also can be mitigating if "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." AG ¶ 17(c). This mitigating condition is not established for the reasons set out above in the discussion of AG ¶ 35(a) under Guideline K.

Finally, security concerns under this guideline can be mitigated if "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" AG ¶ 17(d). Applicant initially acknowledged his misrepresentations to the FSO, but this mitigating condition is not established because he recanted his earlier acknowledgement of intentionally misleading her.

Whole Person Concept

Under the whole person concept, an 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. An 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 common sense judgment based upon careful consideration of the guidelines and the whole person concept. Some of the factors in AG ¶ 2(a) were addressed above, but some warrant additional comment.

Applicant is a mature, highly educated, very intelligent, very articulate person. He has held a clearance for more than 40 years. His security violations in February 2003 were attributable to his lack of training and experience as a security manager and FSO. The organizational structure of his company, although approved by DSS, lacked effective safeguards against inadvertent security violations. It made him the ISSM and FSO, positions for which he had no training or experience. There is no evidence of efforts by DSS to compel Applicant to complete the required training in a timely manner. Since the security violations in February 2003, he has taken corrective action, completed the required training, and has had no further security violations.

Applicant acknowledged his misleading comments to the contractor's FSO and attempted cover-up of his violations until another agency withdrew his eligibility for access to SCI. He then recanted his earlier admissions, and at the hearing he denied intentionally misleading the FSO. While his deceptive conduct with the FSO, standing alone, could be considered an isolated incident, his lack of candor at the hearing causes serious concern about his current reliability and trustworthiness. Although his lack of candor at the hearing is not alleged in the SOR, it may be considered as part of the whole person analysis. ISCR Case No. 03-20327, *supra.*

After weighing the disqualifying and mitigating conditions under Guidelines K and E, and evaluating all the evidence in the context of the whole person, I conclude Applicant has mitigated the security concerns based on handling protected information, but he has not mitigated the security concerns based on personal conduct. Accordingly, I conclude he has not carried his burden of showing that it is clearly consistent with the national interest to continue his eligibility for access to classified information.

Formal Findings

I make the following formal findings for or against Applicant on the allegations set forth in the SOR, as required by Directive ¶ E3.1.25 of Enclosure 3:

Paragraph 1, Guideline K:	FOR APPLICANT
Subparagraphs 1.a-1.c:	For Applicant
Paragraph 2, Guideline E:	AGAINST APPLICANT
Subparagraph 2.a:	For Applicant
Subparagraph 2.b:	Against Applicant
Subparagraph 2.c:	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 continue Applicant's eligibility for a security clearance. Eligibility for access to classified information is denied.

_____
LeRoy F. Foreman
Administrative Judge