DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
----------	)	ISCR Case No. 08-08974
SSN: ----------	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: John B. Glendon, Esq., Department Counsel
For Applicant: Diana J. Veilleux, Esq., and Marian N. Coleman, Esq.

July 22, 2009

Decision

FOREMAN, LeRoy F., Administrative Judge:

This case involves security concerns raised under Guidelines K (Handling Protected Information), M (Use of Information Technology Systems), and E (Personal Conduct). Eligibility for access to classified information is denied.

Statement of the Case

Applicant submitted an application to continue his security clearance on March 14, 2008. On January 27, 2009, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) detailing the basis for its preliminary decision to revoke his clearance, citing security concerns under Guidelines K, M, 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 adjudicative guidelines (AG) promulgated by the President on December 29, 2005.

Applicant received the SOR on January 30, 2009. He answered it through counsel on February 18, 2009; and he requested a hearing before an administrative judge. DOHA received the request on February 19, 2009. Department Counsel was ready to proceed on April 6, 2009, and the case was assigned to me on April 7, 2009. DOHA issued a notice of hearing on April 27, 2009, scheduling the hearing for May 19, 2009. I convened the hearing as scheduled. Government Exhibits (GX) 1 through 11 were admitted in evidence without objection. Applicant testified on his own behalf. The record closed upon adjournment of the hearing on May 19, 2009. DOHA received the transcript (Tr.) on May 27, 2009.

Findings of Fact

Applicant is a 47-year-old staff analyst for a federal contractor. He has held a security clearance since May 2003. He has worked for his current employer since March 2008. He previously worked for another federal contractor for about 22 years. He resigned from his previous employment in lieu of termination and was unemployed from November 2007 until March 2008. The conduct alleged in the SOR occurred while he was working for his previous employer. Applicant testified his current employer is aware of the allegations in the SOR (Tr. 54).

On March 22, 2007, Applicant moved two classified computers from one classified area to another. He obtained the approval of his group leader and deputy group leader in advance, but he did not notify his information systems security officer (ISSO) (GX 4 at 4). He moved the computers because he believed the limitations on network access imposed by the ISSO at the old location limited his ability to do his job (Tr. 65).

On March 29, 2007, Applicant attended a meeting about moving classified computers. He testified this meeting was about computers other than the two he had requested approval to move (Tr. 85), but security investigators found that the meeting was to discuss his requested move (GX 4 at 4). He told an investigator and he testified that he disclosed at the meeting that he had moved his two computers on the day before the meeting (GX 4 at 13). One of the attendees at the meeting told investigators Applicant did not disclose the move of the computers at the meeting (GX 4 at 7).

On March 30, 2007, the computers were discovered to be missing from their old location. When interviewed, Applicant stated he moved the computers on March 28, 2007. Access logs reflected that Applicant entered the secure location to which he had moved the computers on March 22, but not on March 28.

Applicant also told investigators he complied with an informal “two-man rule” for moving classified equipment, and he named the employee who accompanied him. When advised that the employee denied participating in the move, Applicant named a second employee, who also denied participating in the move.

Finally, Applicant stated he carried the two computers in a locked security bag. An employee who observed Applicant entering the new location informed investigators that Applicant was carrying only one computer and it was not in a bag, but the witness admitted he "could not be absolute" about the number of computers Applicant was carrying (GX 4 at 12).

Applicant testified he did not know why he misidentified the person who escorted him during the movement of the computers. He testified he "just got them confused." He denied intending to give the investigators incorrect information (Tr. 48-49).

Applicant testified he realized he had given the wrong date for moving the computers when he was reviewing his statement to the investigators. He explained that he was focused on moving the computers and the date "stuck in [his] head." He could give no other explanation for the discrepancy (Tr. 70-71). He denied intentionally giving false or misleading information to the investigators (Tr. 49-51).

Applicant was first interviewed on May 2, 2007. He did not correct his statement regarding the date he moved the computers until June 7, 2007, when he was confronted with the discrepancies in his first statement. He did not address his misidentification of the person who accompanied him until he was interviewed again on June 18, 2007.

Applicant testified he moved the computers in a locked bag. He testified he is confident he moved the computers in a locked bag because the security officers in the new location would have cited him for a security infraction and refused to accept them if they had been transported incorrectly (Tr. 51-52). However, the security investigation concluded that there was no formal policy on transporting classified computers (GX 4 at 14; Tr. 116).

Although it was "common practice" to notify the ISSO when moving classified computers, there was no formal written guidance requiring it (GX 5 at 3). Applicant testified he was aware of the "two-man rule" but was unaware of other policies regarding movement of computers from one secure area to another. He also testified he did not intend to violate his employer's policies when he moved the computers (Tr. 32). On June 20, 2007, after Applicant moved his computers, an email was distributed announcing a requirement to notify the ISSO when any classified computers are moved (GX 4 at 18-19).

During the inquiry into the move of the two computers, investigators also discovered that Applicant had failed to update his inventory database, failed to obtain ISSO approval for switching disks on classified computers, failed to activate a password screen lock on a classified computer, and failed to mark his media while working in a mixed media environment (GX 4 at 8-9). The computers were in a storeroom and not connected to the network (GX 4 at 6).The investigators concluded there was no suspected unauthorized disclosure of classified information (GX 4 at 4).

Applicant told investigators and testified he believed that the local rules allowed disks to be removed and replaced for testing and maintenance for up to five days without notifying the ISSO and updating the documentation (GX 4 at 26). He testified he could not recall whether he was performing tests or maintenance when he changed the disks on his computer (Tr.38).

Applicant also testified he was required to activate a password screen lock on any computer for which he was responsible. He testified he could not respond specifically to the allegation because he could not determine who was responsible for the computers referred to by the investigators (Tr. 40).

The local rules applicable to the secure local area network required marking of all classified and unclassified media in mixed media work areas (GX 5 at 10). Applicant testified he and the security staff had marked everything in his office "within weeks" before his access was suspended. He testified it was possible that something was overlooked, but he could not determine what improperly marked items the investigators found (Tr. 41).

Applicant's access to classified areas was withdrawn on April 5, 2007 (GX 4 at 5). While the investigation of the moving of computers was ongoing and Applicant's access to classified areas was suspended, he voluntarily underwent retraining in security procedures (Tr. 28).

The local rules applicable to the secure local area network prohibited use of external memory sticks, thumb drives, or similar devices; and they prohibited making any configuration changes to computer systems without prior ISSO approval (GX 5 at 11). On May 9, 2007, a thumb drive was found on the employer's property. Based on a review of the contents on the thumb drive, it was identified as Applicant's property. The thumb drive contained personal photographs, work documents, and a short sexually-explicit video-clip. The work documents were unclassified but were marked Official Use Only (GX 4 at 15).

Applicant told investigators he did not use the thumb drive at work. At the hearing, he testified he sometimes emailed documents from work to his home computer and he used his thumb drive to transfer documents between his home computer and his work computer (Tr. 97-99).

Applicant told investigators he carried the thumb drive with a chain hooked to his belt, and it was lost when the chain broke (GX 4 at 15). At the hearing, he testified he believed he had dropped the thumb drive between two "packets" of his work bag and it dropped out as he was walking from his car to his office. He did not know he had lost the thumb drive until he was notified by security that it had been found. He testified he believed it would have been a security violation to carry the thumb drive into a secured area, but the thumb drive was lost after his access to secured areas had been withdrawn. He testified he had forgotten about the sexually explicit video clip (Tr. 42-45).

Applicant had a reputation for "flying under the radar" regarding security rules and procedures. In March 2006, he violated the organization's "extended security plan" by transferring three classified hard drives from one location to another without notifying anyone (GX 4 at 14). In September 2006, a group administrator complained to Applicant's supervisor about Applicant's lack of cooperation on updating inventories (GX 4 at 8). Applicant's supervisor told security investigators that Applicant had a history of "operating independently from [his organization's] procedures," making his co-workers uncomfortable working with him (GX 4 at 6). Applicant's deputy office director told security investigators Applicant had received several warnings during the past two to three years about his security behavior (GX 4 at 5).

On November 7, 2007, Applicant was notified he was being terminated for cause. The termination notice recited that he exhibited a "cavalier attitude" toward security and a willingness to bend the rules. It also recited that he deliberately provided misleading information to his supervisors and the security investigators (GX 3). Applicant was allowed to resign in lieu of termination (Answer to SOR; GX 2 at 5). He testified he did not file a grievance to "clear his name," because he had no desire to continue working for that employer (Tr. 62). The "Report by Office Concerned" dated November 28, 2007, recited that Applicant "historically had difficulty in adequately following all details involved with security" and had been counseled numerous times (GX 4 at 17).

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 commonsense 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 made "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

SOR ¶ 1.a alleges Applicant's access to classified areas at his place of employment was suspended in March-April 2007 because of his noncompliance with security procedures. SOR ¶ 1.b alleges he acted without authorization and in violation of security procedures when transferring a computer at his place of employment, and he was counseled and retrained in security procedures because of this violation and other unspecified incidents. SOR ¶ 1.c alleges he violated security policies and procedures by bringing a thumb drive onto his place of employment that contained work product and pornography, he lost the thumb drive but did not report its loss, and the thumb drive was found in an unsecure location. SOR ¶ 1.d alleges he was reprimanded, recommended for termination for cause, and escorted from his place of employment because of his violations of rules and regulations and deliberately providing misleading information to his managers and security personnel.

AG ¶ 33 expresses the security concern pertaining to handling protected information: "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 relevant potentially disqualifying conditions are AG ¶ 34(g) ("any failure to comply with rules for the protection of classified or other sensitive information") and AG ¶ 34(h) ("negligence or lax security habits that persist despite counseling by management").

SOR ¶ 1.a does not allege any security violations separate from those alleged in SOR ¶¶ 1.b-1.d. Instead, it merely alleges the actions of his supervisors in response to those violations. It essentially duplicates SOR ¶¶ 1.b-1.d. When the same conduct is alleged twice in the SOR under the same guideline, one of the duplicative allegations should be resolved in Applicant's favor. *See* ISCR Case No. 03-04704 (App. Bd. Sep. 21, 2005) at 3. Accordingly, I resolve SOR ¶ 1.a in Applicant's favor.

Applicant's transfer of his classified computers to a new location raised questions whether he properly notified the appropriate officials of the move and whether he executed the move in accordance with prescribed security procedures. The evidence shows he obtained the approval of his supervisors for the intended move, but he did not notify the ISSO responsible for the computers at the old location. The evidence also shows there was no formal, published rule requiring notification of the ISSO. The requirement for ISSO notification was published after Applicant moved the computers.

Applicant was aware of an informal, unpublished "two-man rule" for moving classified equipment, but his conflicting statements raise a question whether he complied with it. The evidence is also conflicting on the question whether Applicant transported the computers in a locked bag. It is not necessary to resolve these conflicts, however, because the local security procedures did not provide specific guidance for transporting classified computers. The investigators determined that there was no compromise of classified information. Based on this record, I conclude the evidence does not support a finding that Applicant violated any rules when he moved the two computers.[1]

SOR ¶ 1.b also alleges there were "other incidents" of rules violations that resulted in later counseling and retraining. The "other incidents" alleged in SOR ¶ 1.b are supported by substantial evidence of Applicant's failure to update his inventory database, failure to obtain ISSO approval for switching disks, failure to activate a password screen lock, and failure to mark his media.

Applicant testified he believed carrying his thumb drive into a secure area would be a security violation, but he admitted occasional use of the thumb drive to transfer

[1] Applicant's former employer was not an agency under the jurisdiction of the Department of Defense. I cannot determine whether his conduct violated any applicable departmental regulations or directives because no evidence of the rules promulgated by the department having jurisdiction over his former employer was presented.

documents between his home computer and his work computer. The local rules specifically prohibited use of thumb drives without prior ISSO approval. The work documents on the thumb drive were Official Use Only, and as such were "sensitive information" within the meaning of this guideline. Applicant's failure to notice or report the loss of his thumb drive containing sensitive information does not establish a deliberate security violation, but it does indicate negligence.

SOR ¶ 1.d alleges the actions taken by Applicant's supervisors for the violations alleged in of SOR ¶¶ 1.b and 1.c, and it additionally alleges that Applicant deliberately provided misleading information to managers and security personnel. This latter allegation is supported by evidence that when Applicant was interviewed by security investigators he misstated the date he moved the computers, misidentified his escort for the movement of the computers, and denied using the thumb drive at work.

Based on the foregoing, I conclude there is substantial evidence raising the disqualifying conditions in AG ¶¶ 34(g) and (h), shifting the burden to Applicant 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 may be mitigated if "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). The first prong of this mitigating condition ("so much time has elapsed") focuses on whether the conduct was recent. There are no "bright line" rules for determining when conduct is "recent." The determination must be based on a careful evaluation of the totality of the evidence. ISCR Case No. 02-24452 at 6 (App. Bd. Aug. 4, 2004). If the evidence shows "a significant period of time has passed without any evidence of misconduct," then an administrative judge must determine whether that period of time demonstrates "changed circumstances or conduct sufficient to warrant a finding of reform or rehabilitation." *Id*.

More than two years have elapsed since Applicant's security violations. However, he was under investigation and his access to classified materials was suspended until he resigned in lieu of termination in November 2007. He was unemployed from November 2007 until he began his current job in March 2008. Since March 2008, he has been under the pressure of trying to keep his clearance. Under these circumstances, I conclude that Applicant's conduct was "recent" because he has not worked for his current employer long enough to demonstrate reform or rehabilitation.

Applicant has a record of multiple security infractions that did not occur under unusual circumstances. The circumstances under which he left his previous employment cast doubt on his current reliability, trustworthiness, and good judgment. I conclude AG ¶ 35(a) is not established.

Security concerns under this guideline also may be mitigated if "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). Applicant underwent remedial security training, but he has not worked long enough in a classified environment since his resignation in lieu of termination to demonstrate the "positive attitude" required for this mitigating condition.

Finally, security concerns may be mitigated if "the security violations were due to improper or inadequate training." AG ¶ 35(c). The security investigators found a lack of guidance in several areas of security concern, but the guidance was specific and clear regarding marking of media, password protection, and use of external devices such as thumb drives. Applicant's responses during the security investigation and at the hearing demonstrated that he was familiar with the formal, written guidance as well as the informal common practices at his workplace. I conclude AG ¶ 35(c) is not established.

Guideline M, Use of Information Technology Systems

The SOR cross-alleges the same conduct discussed above under this guideline. The concern under this guideline is: "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." AG ¶ 39.

The relevant disqualifying conditions are 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") and AG ¶ 40(g) ("negligence or lax security habits in handling information technology that persist despite counseling by management"). The evidence raises both of these disqualifying conditions.

Security concerns under this guideline may be mitigated if "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" AG 41(a). Applicant's security violations were recent and did not happen under unusual circumstances. His record of multiple violations after repeated counseling precludes a finding that they are unlikely to recur. His record casts doubt on his reliability, trustworthiness, and good judgment. I conclude AG 41(a) is not established. No other enumerated mitigating conditions are relevant.

Guideline E, Personal Conduct

The conduct alleged under Guidelines K and M is also cross-alleged under this guideline. The 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. 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.

The relevant disqualifying condition regarding the information provided by Applicant during the security investigation is "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).

When a falsification allegation is controverted, as in this case, the government has the burden of proving it. A factual misstatement, standing alone, does not prove an applicant's state of mind. An administrative judge must consider the record evidence as a whole to determine whether there is direct or circumstantial evidence concerning an applicant's state of mind at the time of the misstatement. *See* ISCR Case No. 03-09483 at 4 (App. Bd. Nov. 17, 2004).

I found Applicant's explanations for initially misstating the date he moved the computers and the identity of the persons who accompanied him implausible and not credible. Accordingly, I conclude AG ¶ 16(b) is raised.

Security concerns raised by false or misleading answers during a security investigation may be mitigated by showing that "the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts." AG ¶ 17(a). Applicant was first interviewed on May 2, 2007. He did not correct his statement regarding the date he moved the computers until he was questioned on June 7, 2007, and confronted with the discrepancies in his first statement. He did not address his misidentification of the person who accompanied him until he was interviewed on June 18, 2007. AG ¶ 17(a) is not established because Applicant's corrections of his misstatements were not prompt and did not occur until he was confronted with the evidence. No other mitigating conditions are relevant to his statements to security investigators.

The relevant disqualifying conditions for Applicant's security violations are AG ¶¶ 16(c) and (d). AG ¶ 16(c) applies when there is:

> 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) applies when there is:

> 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) condition encompasses "a pattern of dishonesty or rule violations." AG ¶ 16(d)(3). Applicant's security infractions raise AG ¶¶ 16(c) and (d).

Security concerns arising from rules violations may be mitigated 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). Applicant's infractions were numerous and did not happen under unique circumstances. Some of Applicant's infractions were arguably minor, but when considered in totality they cast doubt on his reliability, trustworthiness, and good judgment. I conclude AG ¶ 17(c) is not established.

Security concerns also may 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 has acknowledged some of his infractions. He has attended remedial training and he is working in a new environment. Given his track record, however, I am not satisfied that his behavior is not likely to recur. I conclude AG ¶ 17(c) is not fully established.

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 commonsense judgment based upon careful consideration of the guidelines and the whole person concept. I have incorporated my comments under Guidelines K, M, and E in my whole person analysis. Some of the factors in AG ¶ 2(a) were addressed under those guidelines, but some warrant additional comment.

Applicant is a mature adult who worked for his previous employer for 22 years and held a clearance for many years. The investigation into his move of two classified computers revealed that many security procedures at his previous place of employment were informal, and there no procedures published for certain actions, such as moving classified computers. Nevertheless, Applicant was aware of the informal "two-man rule" and he believed there was a requirement that classified computers be transported in a locked bag. He also was familiar with the published local rules prohibiting use of external devices such as thumb drives. His track record of repeated security lapses and his false responses to security investigators raise serious questions about his current reliability, trustworthiness, and good judgment.

After weighing the disqualifying and mitigating conditions under Guidelines K, M, and E, and evaluating all the evidence in the context of the whole person, I conclude Applicant has not mitigated the security concerns under these guidelines. 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 on the allegations set forth in the SOR, as required by Directive ¶ E3.1.25:

Paragraph 1, Guideline K:	AGAINST APPLICANT
Subparagraph 1.a:	For Applicant
Subparagraph 1.b:	Against Applicant
Subparagraph 1.c:	Against Applicant
Subparagraph 1.d:	Against Applicant
Paragraph 2, Guideline M:	AGAINST APPLICANT
Subparagraph 2.a:	Against Applicant
Paragraph 3, Guideline E:	AGAINST APPLICANT
Subparagraph 3.a:	Against Applicant

Conclusion

In light of all of the circumstances, 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