DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 10-04911
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: David F. Hayes, Esq., Department Counsel
For Applicant: Christopher Graham, Esq.

September 19, 2011

Decision

RIVERA, Juan J., Administrative Judge:

Applicant stored classified documents in a laptop, an external hard drive, and at home in violation of security rules and regulations. He then attempted to conceal his questionable behavior by deleting classified documents from his laptop prior to providing the laptop to Government investigators. He violated the trust and confidence placed in him by the Government. Clearance denied.

Statement of the Case

After reviewing the results of both criminal and security violations investigations, adjudicators for the Defense Office of Hearings and Appeals (DOHA) were unable to make a preliminary affirmative finding[1] that it is clearly consistent with the national interest to grant Applicant's request for a security clearance.

[1] Required by Executive Order 10865, *Safeguarding Classified Information Within Industry,* dated February 20, 1960, as amended; and Department of Defense (DoD) Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (Directive), dated January 2, 1992, as revised.

On December 22, 2010, DOHA issued Applicant a statement of reasons (SOR), identifying security concerns under Guideline K (Handling Protected Information), Guideline E (Personal Conduct), and Guideline M (Use of Information Technology Systems) of the adjudicative guidelines (AG).[2]

On January 20, 2011, Applicant responded to the SOR allegations and requested a hearing before an administrative judge. The case was assigned to me on May 20, 2011, to determine whether a clearance should be granted or denied. DOHA issued a notice of hearing on May 25, 2011, and the hearing was convened as scheduled on June 28, 2011.

The Government offered exhibits (GE) 1 through 8, which were admitted without objection, except for GE 4 that was returned to the Government. I marked as GE 9 for identification, the Government's excerpts of the pertinent security rules and regulations. Applicant testified, presented one witness, and submitted exhibits (AE) 1 through 16, which were admitted without objection, except for AE 11 that was returned to Applicant. I marked as AE 17 for identification a document submitted by Applicant post-hearing. I considered both GE 4 and AE 11 (classified as NATO Restricted documents), as redundant and cumulative to other record evidence. DOHA received the transcript of the hearing (Tr.) on July 11, 2011.

Findings of Fact

Applicant denied all the SOR allegations, except for ¶ 1.a, which he partially admitted. He admitted that he stored two North Atlantic Treaty Organization (NATO) Confidential documents in his house. His admission is incorporated here as a finding of fact. After a thorough review of the evidence of record, and having considered Applicant's demeanor and testimony, I make the following findings of fact.

Applicant is a 61-year-old Government contractor doing business with NATO since 1996. He married his wife in 1982, and they have a 24-year-old son. Applicant was commissioned as a U.S. Army officer in 1971, and served on active duty until his retirement in 1995. He retired as a field grade officer, and his time in service was characterized as honorable. Applicant is a graduate of the Army War College, commanded a battalion during the Gulf War, and served with distinction in several important operational planning positions.

During his military career, Applicant served 13 years overseas, which included several assignments to NATO. He was posted to NATO during his last military assignment prior to his retirement. While in the service, Applicant possessed a top secret security clearance with access to sensitive compartmented information (SCI).

[2] Adjudication of this case is controlled by the AGs, implemented by the DoD on September 1, 2006.

There is no evidence that while in the service Applicant compromised or caused others to compromise classified information.

In 1996, Applicant and his partner established a U.S.-based corporation to provide contractual services to NATO countries. Applicant's secret security clearance was sponsored by the United States. He was afforded access to classified information under the provisions of the National Industrial Security Program (NISPOM). Applicant's company has been successful doing business with NATO. As of the hearing day, it had handled over 300 contracts with NATO.

In February and March 2007, Applicant was holding meetings in offices located within the NATO headquarters building. Both meetings were interrupted by U.S. Army counter-intelligence personnel (investigators) seeking a rogue wireless transmitter communicating with the embassy of a hostile government from within the NATO building. In March 2007, Applicant's laptop was identified as the rogue transmitter. Applicant was asked for permission to inspect his laptop. He initially refused to allow the investigators to inspect his laptop.

On April 17, 2007, Applicant set up an appointment to turn over his laptop to the investigators on April 20, 2007. A subsequent forensic analysis of Applicant's laptop drive revealed that prior to turning over the laptop, Applicant conducted extensive searches and deletions of programs and documents from his laptop. On April 14-17, 2007, Applicant searched his laptop drive seeking any documents containing the terms "confidential" and "secret." He then deleted approximately 200 documents from his laptop drive. On April 18, 2007, he conducted another similar search of his laptop drive and deleted approximately 2,000 documents. (Tr. 252-253)

The forensic analysis also revealed that Applicant backed up his laptop drive onto an external hard drive before deleting the documents. Forensic counter-intelligence investigators recovered 130 of the 2,200 documents Applicant deleted from his laptop. Approximately 100 of the recovered documents were classified NATO Confidential or above. (Tr. 246, AE 16) Three of the documents were identified as NATO secret documents, and two were identified as U.S. secret documents. (AE 16, Tr. 250-252, 273-276)

Applicant had not registered his laptop with NATO authorities, as he was required to do in accordance with NATO information security policies. (GE 3) Nor was he authorized to use a wireless modem from within the NATO building. Applicant registered the laptop with NATO authorities approximately six days after he was asked by the investigators for permission to inspect his laptop.[3] (GE 6) The external hard drive was never registered with NATO authorities, and it was not authorized to handle NATO classified documents. (Tr. 247) Applicant transferred U.S. and NATO classified

[3] According to the investigation report, the investigators searching for the rogue transmitter asked Applicant whether his laptop was registered with NATO, and he answered "Yes." The laptop was not registered with NATO authorities until six days later.

documents from the laptop to his external hard drive prior to deleting the documents from his laptop, and before he provided the laptop to investigators. The external hard drive with the classified documents was unsecured for approximately 14 months. (GE 3) Although Applicant possessed a U.S. secret clearance, and was authorized access to classified information up to NATO secret, he was not authorized to store documents classified NATO Confidential, NATO Secret, or U.S. Secret in his laptop, hard drive, or at his home. During the 2007 criminal investigation, Applicant admitted to knowingly loading and storing classified documents in his laptop without authorization. (GE 3)

As a U.S.-sponsored contractor doing business with NATO, Applicant was required to update his U.S. security clearance yearly, to participate in yearly security clearance briefings, and to follow the NISPOM and NATO security procedures for the handling of classified information and documents. (Tr. 190, AE 11) In August 2005, Applicant signed a Personnel Security Clearance Form, stating that he had been briefed and understood the principles and regulations for handling and safeguarding NATO classified materials. (GE 3)

On March 8, 2008, Applicant was arrested and charged with espionage by the host nation government. A search of his home revealed that he had stored in his home 38 hard copies of classified documents. Applicant was not authorized to store at his home or to possess documents classified above the NATO Restricted classification. After a two-year criminal investigation, it was determined that no hostile intelligence services were involved, and the criminal charges were dismissed. In July-August 2008, Applicant's access to NATO classified information was suspended because of his security violations and he was barred from NATO premises.

At his hearing, Applicant admitted that prior to turning over his laptop to the investigators, he performed extensive searches for documents containing the words "confidential" and "secret." He claimed he was surprised to find such documents in his laptop, and that he deleted them pursuant to NISPOM and NATO security procedures. He stated most of the documents were uploaded to his laptop, without his knowledge, during a March 2005 deployment when his laptop was used as the repository for documents produced during the deployment. He claimed that he informed the general officer in charge of the deployed NATO unit that his laptop was only cleared to handle NATO Restricted documents. As a field expediency measure, the general officer authorized him to store NATO Confidential documents in his laptop. (Tr. 104-105; 142-159)

After Applicant returned from his deployment, he did not delete from his laptop documents beyond the laptop accreditation. Nor did he notify security personnel that he had documents in his laptop beyond the laptop's classification. Applicant admitted that he connected his laptop, which contained classified information, to commercial internet providers. At his hearing, he claimed that at the time of the internet connections, he was not aware the laptop contained classified documents. Applicant's connections with commercial internet providers made the classified information vulnerable to compromise.

Applicant expressed remorse for storing and possessing documents beyond his and the laptop's accreditation. He averred some of the documents were improperly classified, and that NATO has systemic problems declassifying documents. He claimed some of the documents' classifications had been downgraded; however, he did not present documentary evidence to support his claims. Applicant also claimed NATO did not provide him with the training needed for him to properly deal with classified documents. Applicant averred he always "played by the rules," and that he never had any security violations before this incident.

Applicant testified that as a result of the criminal investigation against him, and the ongoing security clearance process, he now has a better understanding of his responsibilities for handling classified documents. His company implemented changes and is training its employees in the handling of classified information and security procedures to avoid similar issues.

Policies

The President of the United States 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. *Department of the Navy v. Egan*, 484 U.S. 518, 527 (1988). The President has authorized the Secretary of Defense to grant 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. The U.S. Supreme Court has recognized the substantial discretion of the Executive Branch in regulating access to information pertaining to national security, emphasizing that "no one has a 'right' to a security clearance." *Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988).

Eligibility for a security clearance is predicated upon the applicant meeting the criteria contained in the adjudicative guidelines. These AGs 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 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 to reach his decision.

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 that the applicant may deliberately or inadvertently fail to safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation of potential, rather than actual, risk of compromise of classified information. 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. *See also* Executive Order 12968 (Aug. 2, 1995), Section 3. Thus, nothing in this Decision should be construed to suggest that I have based this decision, in whole or in part, on any expressed or implied determination about Applicant's allegiance, loyalty, or patriotism. It is merely an indication that 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 and an applicant's security suitability. *See* ISCR Case No. 95-0611 at 2 (App. Bd. May 2, 1996); and ISCR Case 08-06605 at 3 (App. Bd. Feb. 4, 2010).

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 or her] security clearance." ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002). The burden of disproving a mitigating condition never shifts to the Government. *See* ISCR Case No. 02-31154 at 5 (App. Bd. Sep. 22, 2005). "[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

The facts and circumstances raising security clearance concerns under Guidelines K, E, and M are substantially the same, with some exceptions. For the sake of brevity, they will be articulated under the Guideline K discussion, and incorporated by reference into the discussions under Guidelines E and M. The exceptions will be discussed in the pertinent guideline.

Guideline K, Handling Protected Information

AG ¶ 33 articulates the security concern relating to handling classified 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.

Applicant uploaded and stored NATO Confidential, NATO Secret, and U.S. Secret documents in a laptop that was not registered with NATO authorities and not

cleared for the handling of classified documents. He failed to safeguard the classified information when he accessed commercial internet providers while the laptop contained the classified documents. Applicant also uploaded and stored NATO and U.S. classified information on an external hard drive that was not registered or cleared for such information. The external hard drive was unsecured for 14 months.

Before providing over his laptop to Government investigators in April 2007, Applicant conducted extensive searches for documents containing the terms "confidential" and "secret." He then deleted approximately 2,200 files from his laptop. Government forensic investigators recovered approximately 130 documents classified NATO Confidential or above from his laptop and external hard drive. Three of the recovered documents were classified NATO Secret and two were classified as U.S. Secret documents. Additionally, Applicant stored in his home hard copies of 38 NATO and U.S. classified documents in violation of security rules and regulations.

AG ¶ 34 provides three disqualifying conditions that raise a security concern and are disqualifying in this case:

> (b) collecting or storing classified or other protected information at home or in any other unauthorized location;
>
> (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, word processor, or computer hardware, software, drive, system, gameboard, handheld, "palm" or pocket device or other adjunct equipment; and
>
> (g) any failure to comply with rules for the protection of classified or other sensitive information.

AG ¶ 35 provides three mitigating conditions that could mitigate the Guideline K security concerns:

> (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;
>
> (b) the individual responded favorably to counseling or remedial security training and now demonstrates a positive attitude toward the discharge of security responsibilities; and
>
> (c) the security violations were due to improper or inadequate training.

Mitigating conditions AG ¶¶ 35(a) and (b) are partially applicable, but do not fully mitigate the security concerns. Applicant's questionable behavior stopped in 2007, as a

result of a Government investigation. As such, it could be considered temporally remote. Notwithstanding, considering the evidence as a whole, I find Applicant knowingly and willfully violated security rules and regulations. The security violations did not occur under unusual circumstances, and they continued during a long period. In light of Applicant's maturity, education, and his extensive experience as a U.S. Army officer and NATO contractor, his past behavior continues to cast doubt on Applicant's current reliability, trustworthiness, and judgment.

I considered Applicant's claims about his lack of training handling NATO classified documents; that some of the documents were improperly classified or have been declassified; and that a general officer authorized him to store classified documents in his laptop as a result of field expedience. I find Applicant's explanations and claims not to be credible. As stated above, Applicant served in the U.S. Army as an officer in high-level, operational and planning positions. He was trained in the proper procedures for handling U.S. classified documents. The same basic security principles, rules and procedures he learned in the Army to handle classified documents applied to his handling of NATO classified documents. He was aware of U.S. and NATO security rules and procedures because of his years of military service, his assignment to NATO, his annual security briefings, and his experience as a U.S. Government contractor with NATO since 1996.

Applicant testified that as a result of the investigation against him, he studied and is now aware of NATO security rules and regulations. He claimed that he now has a positive attitude toward the discharge of his security responsibilities, and he promised not to make the same mistakes in the future. Notwithstanding, I consider his security violations as serious offenses. Applicant knowingly and willfully violated security rules and procedures by uploading classified documents into both an unregistered laptop and an external hard drive, and by storing classified materials at home. Because of his education, age, and experience, Applicant's actions are not mitigated. Considering the totality of the circumstances, his gross violations of security rules and regulations still raise serious security concerns.

Guideline E, Personal Conduct

AG ¶ 15 explains why personal conduct is a security concern stating:

> 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.

In addition to cross-alleging that Applicant violated NATO and U.S. security rules and regulations, the Government alleged under SOR ¶ 2.a that Applicant attempted to

conceal his unauthorized storage of classified information by deleting and overwriting the documents before providing his laptop to Government investigators.

Applicant claimed that he had no knowledge that he had documents above his laptop classification stored in his laptop. When he conducted the searches and found the documents, Applicant claimed he destroyed the documents in accordance to NATO and NISPOM procedures. Applicant's claims are not credible. Applicant's laptop was not registered with NATO authorities until six days after he was asked by Government investigators for permission to inspect his laptop. Additionally, Applicant provided contradictory testimony. He testified that during a 2005 deployment he was asked to store documents beyond his laptop classification as a field expediency measure. Thus, he knew he had classified documents in his laptop. Furthermore, at his hearing, Applicant acknowledged that he failed to remove those documents from his laptop when the deployment was over, or to disclose to security authorities that he had unauthorized documents in his laptop.

Applicant's initial refusal to provide his laptop to investigators and his searches for documents containing the terms "confidential" and "secret" show that he was aware that he had stored such documents in his laptop. His deleting and overwriting of 2,200 documents hours before providing the computer to investigators, coupled with his failure to disclose to the investigators that he had stored the classified documents in his laptop, demonstrate his intent to conceal his actions. Approximately 100 documents above the laptop's clearance authorization were recovered by forensic investigators. It was not established that the classified documents were all from the 2005 deployment. I note that some of the documents have dates preceding and after the deployment.

SOR ¶ 2.b alleged that around July 2008, Applicant's NATO access to classified information was suspended and that he was barred from NATO premises. This paragraph does not allege any additional security-related misconduct by Applicant. It only states the actions were taken by NATO as a result of Applicant's misconduct. I find for Applicant on this allegation.

Considering the evidence as a whole, I find Applicant's questionable behavior violated:

> AG ¶ 16(e): personal conduct, or concealment of information about one's conduct, that creates a vulnerability to exploitation, manipulation, or duress, such as (1) engaging in activities which, if known, may affect the person's personal, professional, or community standing, or (2) while in another country, engaging in any activity that is illegal in that country or that is legal in that country but illegal in the United States and may serve as a basis for exploitation or pressure by the foreign security or intelligence service or other group.

AG ¶ 17 lists seven conditions that could potentially mitigate the personal conduct security concerns:

(a) the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts;

(b) the refusal or failure to cooperate, omission, or concealment was caused or significantly contributed to by improper or inadequate advice of authorized personnel or legal counsel advising or instructing the individual specifically concerning the security clearance process. Upon being made aware of the requirement to cooperate or provide the information, the individual cooperated fully and truthfully;

(c) the offense is so minor, or so much time has passed, or the behavior is so infrequent, or it happened under such unique circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment;

(d) 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;

(e) the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress;

(f) the information was unsubstantiated or from a source of questionable reliability; and

(g) association with persons involved in criminal activity has ceased or occurs under circumstances that do not cast doubt upon the individual's reliability, trustworthiness, judgment, or willingness to comply with rules and regulations.

Having considered all the mitigating conditions, I find that none apply. Applicant did not disclose his questionable behavior before he was confronted with the facts. To the contrary, the evidence shows he attempted to conceal his security violations. AG ¶ 17(a) does not apply. AG ¶¶ 17(b), (f), and (g) are not raised by the record evidence, and therefore are not relevant. For the same reasons discussed under Guideline K (incorporated herein), mitigating condition AG ¶ 17(c) does not apply. Applicant's behavior is a serious violation of security rules and procedures. His behavior did not occur under unique circumstances, but as a result of Applicant's willful violation of security procedures. As such, it still casts doubt on Applicant's reliability, trustworthiness and judgment.

AG ¶¶ 17(d) and (e) partially apply, but do not fully mitigate the security concerns. Applicant's questionable behavior stopped in 2007, as a result of the criminal investigation and the suspension of his clearance. Applicant claimed he has trained

himself in the proper handling of classified information, and his company has implemented procedures to prevent a similar situation in the future. Applicant expressed remorse for his past behavior. He promised to safeguard classified information in the future. Notwithstanding, because of his education, age, and work experience holding a security clearance, Applicant's willful, repeated, and serious violations of security rules and regulations are not mitigated. Considering the totality of the circumstances, his security violations still raise serious security concerns about his trustworthiness, reliability, and judgment.

Guideline M, Use of Information Technology Systems

AG ¶ 39 articulates the security concern about the misuse of information technology systems:

> Noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual's reliability and trustworthiness, calling into question the willingness or ability to properly protect sensitive systems, networks, and information. Information Technology Systems include all related computer hardware, software, firmware, and data used for the communication, transmission, processing, manipulation, storage, or protection of information.

Applicant's questionable behavior, as discussed under Guidelines K and E, also raise security concerns under AG ¶ 40(d) "downloading, storing, or transmitting classified information on or to any unauthorized software, hardware, or information technology system."

AG ¶ 41 provides three potentially applicable mitigating conditions to the use of information technology systems concern:

> (a) so much time has elapsed since the behavior happened, or it happened under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment;
>
> (b) the misuse was minor and done only in the interest of organizational efficiency and effectiveness, such as letting another person use one's password or computer when no other timely alternative was readily available; and
>
> (c) the conduct was unintentional or inadvertent and was followed by a prompt, good-faith effort to correct the situation and by notification of supervisor.

For the same reasons discussed under the Guidelines K and E mitigating conditions, incorporated herein, I find that none of the mitigating conditions apply.

Whole-Person Concept

Under the whole-person concept, the administrative judge must evaluate an applicant's eligibility for a security clearance by considering the totality of the applicant's conduct and all the relevant circumstances. The administrative judge should consider the nine adjudicative process factors listed at AG ¶ 2(a):

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

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. AG ¶ 2(c). I have incorporated my comments under Guidelines K, E, and M in my whole-person analysis. Some of the factors in AG ¶ 2(c) were previously addressed under those guidelines, but some warrant additional comment.

Applicant honorably served 24 years on active duty in the U.S. Army. He commanded a battalion during the Gulf War, served in important operational planning positions, and possessed a top secret clearance during his service without any incidents. He served 13 years overseas, and his last assignment was at NATO. After his retirement, Applicant established a successful company and has performed over 300 contracts for NATO countries. Applicant expressed remorse for his past behavior. He educated himself in the rules and procedures for the handling of classified information. He promised to discharge his security responsibilities and avoid future violations.

Notwithstanding, the factors in support of not granting Applicant's security clearance are much stronger. During his military career, Applicant was trained in the proper procedures for handling classified documents. The same basic rules and procedures he used in the Army to safeguard classified information applied to his handling of NATO classified documents. He was aware of U.S. and NATO security rules and procedures because of his years of military service, his assignment to NATO, and his 11 years of experience performing contracts for NATO.

Applicant's security violations are serious offenses. His actions established a pattern of violations in the handling of classified information. He aggravated his circumstances when he attempted to conceal his questionable behavior by deleting

classified documents from his laptop prior to providing the laptop to Government investigators. His overall behavior violated the trust and confidence placed in him by the Government. Because of his education, age, and experience, Applicant's actions are not excusable as mistakes caused by inexperience or lack of training. Considering the totality of the circumstances, Applicant's security violations were knowing and willful. His actions raise security concerns about his current judgment, reliability, and trustworthiness.

Formal Findings

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

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

Conclusion

In light of all the circumstances presented by the record in this case, it is not clearly consistent with the national interest to grant or continue eligibility for a security clearance for Applicant. Eligibility for a security clearance is denied.

_____
JUAN J. RIVERA
Administrative Judge