DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
	)	ISCR Case No. 11-05079
	)	
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Marc G. Laverdiere, Esquire, Department Counsel
For Applicant: *Pro se*

02/21/2012

Decision

MATCHINSKI, Elizabeth M., Administrative Judge:

While on duty conducting threat vulnerability assessments for the United States military in June 2004, Applicant lost a notebook containing sensitive information, which he surmises may have been taken by a Russian woman, with whom he engaged in sexual activities in his hotel room. Applicant did not report the loss of the notebook until after he was administered a polygraph examination in January 2009. His exercise of extremely poor judgment is not fully mitigated despite the passage of time. Clearance denied.

Statement of the Case

On September 12, 2011, the Defense Office of Hearings and Appeals (DOHA) issued a Statement of Reasons (SOR) to Applicant, detailing the security concerns under Guideline K, Handling Protected Information, and Guideline E, Personal Conduct, which provided the basis for its preliminary decision to deny or revoke his security clearance. DOHA took the action 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) effective within the Department of Defense on September 1, 2006.

Applicant filed an undated Answer to the SOR allegations, which was received by DOHA on October 26, 2011. He requested a hearing, and on November 23, 2011, the case was assigned to me to conduct a hearing to consider whether it is clearly consistent with the national interest to grant or continue a security clearance for him. On November 30, 2011, I scheduled a hearing for December 21, 2011.

At the hearing, six Government exhibits (GE 1-6) were admitted; GE 3 over Applicant's objections.[1] Seven Applicant exhibits (AE A-G) were entered into evidence. Exhibit A, a personal statement from Applicant, was admitted over the Government's objections about it being testimonial in nature. Applicant and a retired chief warrant officer, who served with Applicant in Southwest Asia, testified on Applicant's behalf, as reflected in a transcript (Tr.) received on December 31, 2011.

Findings of Fact

The SOR alleges under Guideline K (SOR 1.a) and Guideline E (SOR 2.a) that while on active duty conducting threat vulnerability assessments for the U.S. military in June 2004, Applicant failed to safeguard classified notes, thereby violating information security program regulations pertaining to safeguarding working papers, handcarrying classified information, storing classified information, and reporting the loss or compromise of classified information. Applicant denies that he failed to safeguard classified notes transcribed while on official duty or that he violated any security regulations. After considering the pleadings, exhibits, and transcript, I make the following findings of fact.

Applicant is a 35-year-old first-year law student,[2] who is being sponsored for a Top Secret security clearance and sensitive compartmented information access

[1]Government exhibit (GE) 3 contains redacted documents from a 2009 polygraph examination conducted in Southwest Asia, including the examiner's summary and a signed statement from Applicant taken during a polygraph interview. Applicant objected on the basis that the polygraph was unauthorized, in that it was ordered by a military investigator and not in the ordinary course of business. Applicant maintained at his hearing and previously during a subject interview of April 7, 2010, that the military's criminal investigative service had been advised by its headquarters not to polygraph any U.S. citizens. (GE 5; Tr. 18.) However, GE 3 indicates on its face that Applicant required the polygraph examination for special program access while deployed, and that approval was obtained for the test. Applicant presented no documentation substantiating his assertion. Expedited testing was apparently requested. (GE 4.) Applicant also objected to GE 3 on the basis that he was deprived of the opportunity to have an expert assess the results of the examination. With due consideration to Applicant's inability to cross-examine the polygraph examiner, the document does not contain the polygraph questions or results. Applicant's signed statement, which is included in GE 3, is admissible under Federal Rule of Evidence 801.

[2]In September 2011, Applicant was awarded his bachelor's degree, Magna Cum Laude, in legal studies and political science. He was accepted to law school, and had just finished his first semester as of his hearing in December 2011. (AE A, B.)

(TS/SCI), so that they he can be placed on defense contracts. (Tr. 93.) Applicant was initially granted TS/SCI access for his military duties in counterintelligence. His classified access was apparently suspended in February 2009, while he was employed as a senior analyst by a defense consulting firm. (GE 1, 2, 4; AE A.)

Applicant graduated from high school in June 1994. In August 1994, he enlisted in the United States military. For the first four years, he served as a field artillery cannoneer and administrative clerk. In August 1998, he began serving as a counterintelligence/human intelligence (CI/HUMINT) specialist. (AE A, B, C; Tr. 48.) While stationed in a CI/HUMINT command, Applicant was granted TS/SCI access on September 26, 2000. (GE 5; AE A.) Applicant was responsible for writing counterintelligence estimates classified at the Secret/NOFORN (no foreign dissemination) level, and he had no security incidents regarding the handling of classified information. (Tr. 49.) Stationed in the Persian Gulf region starting in June 2002, Applicant primarily conducted HUMINT operations in theater (war zone) from January 2003 until August 2003. (AE B.) Secret/NOFORN information was processed onto field message books, which were kept on his person in very difficult field conditions. Classified reports and removable hard drives were secured in a one-drawer GSA-approved safe attached to a vehicle axel or to a stanchion in a building when available. (AE A; Tr. 50-51.)

In August 2003, Applicant was detailed to a joint counterintelligence support element where he conducted threat vulnerability assessments in Southwest Asia, Africa, and the Middle East. (AE A, B.) He kept separate notebooks for each assignment in which he recorded his observations, usually in shorthand, and he did not conspicuously mark or date them. (AE A; Tr. 56.) Notes were not secured, because according to Applicant, they were unclassified unless combined with information regarding terrorist techniques and procedures. (Tr. 59.) Applicant typically carried the GSA-approved container that held his team's classified computer drives and other classified materials that they were required to transport on trips to conduct threat vulnerability assessments. (AE A; Tr. 59.) He had access to TS/SCI information and received a Joint Meritorious Commendation Medal for his service. From October 2004 to November 2006, Applicant was assigned to a military intelligence activity. (AE A, B, C.) His primary duty area was inside a sensitive compartmented information facility (SCIF), and he was not involved in any security incidents. (AE A; Tr. 51-52.)

On November 5, 2006, Applicant was honorably discharged from active duty at the rank of staff sergeant. He had received several military awards and decorations during his 12 years on active duty. (AE C.) His TS/SCI access was renewed on July 2, 2007, for his duties as an instructor in CI/HUMINT collection techniques for a consulting company (company X) in Southwest Asia from October 2006 to June 2008 (AE B), although he accessed information classified only to the Secret/NOFORN level. (GE 1; AE A; Tr. 52.)

Applicant worked as a consultant screener on a NATO contract with a NATO Secret clearance in Southwest Asia from July 2008 until October 2008 (Tr. 52-53), when

he was rehired by company X. (GE 1, 4, 5; AE A, B.) Expedited determination of Applicant's eligibility for SCI was requested so that he could be assigned as a senior intelligence analyst on a DOD contract in theater. (Tr. 53.) Applicant worked in a hostile environment for about a month and then took a planned two-week vacation in the United States. (Tr. 53.) On January 28, 2009, Applicant was administered a counterintelligence polygraph examination in Southwest Asia by a special agent with a military criminal investigative service.[3] The test was reportedly approved through the criminal investigative service agency's headquarters. (GE 3, 4.)

During a post-polygraph interview, Applicant disclosed to the special agent that while he was assigned to perform a threat vulnerability assessment of U.S. installations in the Persian Gulf region in June 2004, he became acquainted with a woman from Russia at a hotel bar. Over the course of a few hours spent at the bar, Applicant consumed seven or eight alcoholic drinks.[4] At his invitation, Applicant and this foreign woman then took a taxi to his hotel, where they had consensual sexual relations in his room. They "hung out for a while longer-maybe one hour." During this time, Applicant left the Russian woman unsupervised at one point while he was in the restroom. After she left his hotel room, he never saw her again. The next morning, Applicant could not find his notebook, which contained his sensitive observations relating to threat vulnerabilities of U.S. facilities in the area. While he did not recall for certain, he assumed he had the notebook in his possession when he went out the previous evening, because he always kept the notebook in his travel backpack. He "looked everywhere [he] could think of for the notebook,"[5] and when it did not turn up, he suspected that the Russian woman had taken his notebook while he was in the restroom. Applicant admitted to the polygraph examiner that the information in the notebook was considered classified Secret when compiled in a report, and he had not reported the incident to anyone because he was embarrassed that it happened. Applicant acknowledged that even though he was not certain that his notebook had been stolen by the foreigner, he knew that he had lost sensitive information, and that he should have reported the incident "to ensure a timely damage assessment of the material lost." (GE 3, 4; Tr. 74-77.) Applicant provided a statement for the investigator, writing most of it himself, describing the incident. (GE 3, 4; AE A.) At that point, polygraph testing was discontinued before it could be completed due to the examiner's schedule. (GE 3, 4.) Applicant was removed from the DOD contract and sent back to the United States. (GE 4.)

[3]Applicant willingly took the polygraph, although he now asserts that had he known "what the conditions were going to be and such, [he] would have waited until [he] got back to the United States to be in more—less hostile conditions than [they] were in." (Tr. 54-55.) Whatever problems there may have been about the polygraph examination itself (Tr. 64-65), no findings are made or conclusions drawn based on the instrument portion of the polygraph examination.

[4]Applicant denies that he was drunk, although he admits that he was "slightly buzzed." (GE 3, 4.)

[5]Applicant testified at his hearing that he did not check to see that he had everything in his bag before he left his hotel. He did not discover the notebook was missing until he was already with his team and "probably on the next site." (Tr. 81.)

In February 2009, Applicant's TS/SCI access was apparently suspended, and he was terminated from his employment with company X because he was denied access to the defense agency's facilities. (GE 1, 2, 4, 5.) The pertinent defense agency referred investigative jurisdiction to the military criminal investigative service that had conducted the polygraph. In turn, his case was forwarded to a field office for appropriate follow-up action. (GE 2, 3, 4.) There is no evidence that any action was taken before the issuance of the SOR.

In March 2009, Applicant was hired by another defense contractor (company Y) to work as an instructor for a military counterintelligence training program that required him to hold a TS/SCI clearance. (AE B.) When his case had not been adjudicated by September 2009, he was issued a lack of work statement and terminated from employment. (GE 1, 5; AE A.) His former team leader in that job considers the loss of Applicant's services in counterintelligence to be a "loss to the protection of national security interests." Applicant had access to company proprietary data in that job and trust never became an issue. (AE G.)

Applicant collected unemployment until January 2010, when he returned to college to complete his bachelor's degree. (GE 5; AE B.) On February 15, 2010, Applicant completed an Electronic Questionnaire for Investigations Processing (e-QIP) at the request of a potential future employer seeking clarification of his security eligibility. Applicant provided an extensive explanation of the circumstances surrounding the January 2009 polygraph examination conducted in theatre, his termination from company X for reason of his clearance being suspended by the DOD, and another defense contractor's inability to have his security clearance eligibility re-adjudicated. Applicant explained that he had filed Freedom of Information Act (FOIA) requests for information about his clearance, and that he was told that his clearance had been suspended because of company X's failure to have his polygraph examination completed. Applicant expressed a willingness to take another polygraph to clear up the situation. (GE 1.)

On March 16, 2010, Applicant was contacted by telephone by an authorized investigator for the Office of Personnel Management (OPM). Applicant admitted that the woman with whom he had sexual relations in June 2004 was a Russian national, and that he left his job with a defense contractor around September 18, 2009, because he needed a TS/SCI clearance for the contract, and his clearance was not completed. On April 7, 2010, the investigator interviewed Applicant in person about foreign influence and the suspension of his classified access. Applicant asserted that the polygraph examination administered to him in January 2009 was unauthorized, and that only two of three scheduled examinations had been completed. Applicant admitted that he had sex with a female foreign national in his hotel room in 2004, and that he believed he was missing a notebook containing information regarding threat capabilities written in shorthand form (abbreviated notes) with key words to prompt his thoughts containing the details. Applicant denied that the information in the notebook was classified or that it was useful to anyone. While he acknowledged he had not found the notebook, he felt it could have been lost elsewhere. He further asserted that he did not see the significance

of reporting the information at the time, but he planned to report any such information in the future. He denied any other occasion in which his actions could have possibly resulted in the compromise of duties or of classified information. As of April 2010, he had not been formally notified by the DOD of his clearance suspension. (GE 5.)

In the summer of 2010, in response to separate FOIA requests, Applicant was provided a copy of his January 28, 2009, statement to the criminal investigative service special agent, which he then provided to DOHA. (GE 2, 3, 4.) A summary completed by the criminal investigative service indicates that Applicant had admitted in his interview "to the loss of classified information." (GE 3.) Applicant denies that the notebook contained any classified material, and that any of the regulations pertinent to safeguarding classified information applied to such notebooks:

> The notebook contained my handwritten observations made while performing security assessments if certain structures and other buildings. These observations were written in a shorthand and cryptic manner, making them almost unintelligible to anyone who found them. Accordingly, standing alone, these notes did not constitute classified material. Rather, they only became classified once combined with other information. Several of my former colleagues in the [military] also conducted similar security assessments and took notes in notebooks in the same way that I did. None of them understood their notes to constitute classified information, and none of them believed that the various regulations concerning the safekeeping of classified information ever applied to their notebooks. In fact, many of the guidelines concerning the safeguarding of classified materials are not even applicable in the field, or, are processes or methods that were even available for us to use. (AE A.)

As for the June 2004 assignment, Applicant arrived in the country three to five days earlier. Due to poor coordination, he ended up assessing only two or three hotels before moving on to the city where the notebook went missing. In that city, he looked at two areas around the port, which "wasn't really all that exciting." The information in the notebook was not collected from any HUMINT source, but was instead his personal observations, which he maintains were unclassified. (Tr. 62-63.)

In retrospect, Applicant realizes that he "probably" should have notified his command of the missing notebook. He surmises that had he done so, his command would have "just put a little mark in [his] record" and told him to use better judgment. (Tr. 70.) He admits he did not report the loss of the notebook because he was embarrassed and also not sure whether he lost it at first. (Tr. 73, 77-78.)

Applicant is known to be a conscientious, knowledgeable professional by those persons who had the opportunity to observe his performance at various times during his career in counterintelligence. A retired chief warrant officer, with 17 years of experience in counterintelligence and human intelligence, worked alongside Applicant for five months in the Persian Gulf, and otherwise had weekly or semi-weekly contact with

Applicant while both were stationed in the region between 2002 and late 2004. He found Applicant to be very responsible in carrying out intelligence operations. He knows Applicant had a polygraph in which he was questioned about a missing notebook containing his observations while performing vulnerability assessments. He would be willing to work with Applicant in the future in an operational environment that involved classified information. (Tr. 31-33.) In the event that notes containing vulnerability assessment observations were missing, this retired intelligence officer would expect the command to be notified, although he also testified that there would be no reason to report anything if the information in the notebook was not classified. (Tr. 34-35) He admitted that his opinion in this regard could change depending on what other information was available:

> It would depend on what other information is out there that when you combine the two will lead to the classification of the initial or the information in the book. And when we do threat assessments, basically you are looking for observations of the facility, the gate, the wall, that sort of stuff, and you take notes about what you looked at and you don't really explain in the book as to why, that comes later on when you type up your report and you emphasize the reason why something is broken and needs to be fixed. (Tr. 36-37.)

The witness knew of no regulation that covers notes taken from observations, although he also testified that the responsibility for determining the classification of such observations should lie with the individual who wrote the notes because he or she is familiar with the contents. (Tr. 36.) Operational procedure was to bring such notes to the office and secure them in a safe. However, there was no requirement to keep unclassified notes on one's person at all times when on travel or away from the office ("they stay with your backpack or your room"). (Tr. 39.)

A current employee of company Y first became acquainted with Applicant in September 2003, when both he and Applicant provided vulnerability assessments for a joint security directorate. Then a "young and inexperienced counterintelligence specialist," he relied on Applicant often for guidance in operational security matters during missions that forced them to operate in foreign environments outside of secure military installations. Information collected in the course of assessments was safeguarded through "a commonsense approach that mitigated risk of information compromise." Applicant frequently volunteered for, and was trusted with maintaining control of the hard drives, including those which were classified; the thumb drives; and the digital cameras utilized for assessments. It was common practice, and a basic skill learned in counterintelligence training, for cryptic notes to be taken to assist the team members later when they prepared their assessments in a classified area.[6] This character reference characterized the notes as "nothing more than cryptic reminders of items to address in our finished products." Without information of their context or

[6] The use of cryptic notes was a common technique among counterintelligence specialists to "mitigate the risk of potentially sensitive, non-classified information being compromised when operating outside of secure facilities for extended periods of time." (AE D.)

associated photography the notes were virtually useless in the unlikely event they were compromised. In his experience, it was common for team members to leave their personal notebooks in their hotel rooms "tucked away in a suitcase as they would store any personal items or information." In contrast, drafts or finished reports were only written on computer systems under full accountability. This counterintelligence professional has no concerns about Applicant's character or his ability to safeguard unclassified sensitive information or classified information. (AE D.)

Another former military CI/HUMINT specialist, who currently works in the field as a civilian, has known Applicant personally and professionally since 2005. Familiar with Applicant's reputation in the intelligence arena, he attests to Applicant being "well versed in policy, regulation, and the execution of standards of practice in handling classified information." He found Applicant to be "a constant critic of existing regulations and practices which he himself deemed insufficient, despite adherence to existing protocol." He is of the opinion that Applicant effected change in policy and practice in their military unit to improve information and operational security. In their social interactions, Applicant exhibited "the highest character in his decision making and personal control." (AE F.)

A counterintelligence analyst, who worked closely with Applicant in theater from November 2008 until late January 2009, attests to Applicant's "dedication to a job well-done" from the start of his deployment to the hostile environment. In her opinion, Applicant has been subjected to "the unwarranted derision and unfounded suspicions of those who did not know him well enough to know that the suspension of his clearance was an egregious and nightmarish mistake." She considers Applicant to be trustworthy, reliable, and principled person, and recommends him wholeheartedly for classified access. (AE E.)

Policies

The U.S. Supreme Court has recognized the substantial discretion the Executive Branch has 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). When evaluating an applicant's suitability for a security clearance, the administrative judge must consider the adjudicative guidelines. In addition to brief introductory explanations for each guideline, the adjudicative guidelines list potentially disqualifying conditions and mitigating conditions, which are required to be considered in evaluating an applicant's eligibility for access to classified information. These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, these guidelines are applied in conjunction with the factors listed in the adjudicative process. The administrative judge's overall adjudicative goal is a fair, impartial, and commonsense decision. According to AG ¶ 2(c), the entire process is a conscientious scrutiny of a number of variables known as the "whole-person concept." The administrative judge must consider all available, reliable information about the person, past and present, favorable and unfavorable, in making a decision.

The protection of the national security is the paramount consideration. AG ¶ 2(b) requires that "[a]ny doubt concerning personnel being considered for access to classified information will be resolved in favor of national security." In reaching this decision, I have drawn only those conclusions that are reasonable, logical, and based on the evidence contained in the record. Under Directive ¶ E3.1.14, the Government must present evidence to establish controverted facts alleged in the SOR. Under Directive ¶ E3.1.15, the applicant is responsible for presenting "witnesses and other evidence to rebut, explain, extenuate, or mitigate facts admitted by applicant or proven by Department Counsel. . . ." The applicant has the ultimate burden of persuasion to obtain a favorable security decision.

A person who seeks access to classified information enters into a fiduciary relationship with the Government predicated upon trust and confidence. This relationship transcends normal duty hours and endures throughout off-duty hours. The Government reposes a high degree of trust and confidence in individuals to whom it grants access to classified information. 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 as to potential, rather than actual, risk of compromise of classified information. Section 7 of Executive Order 10865 provides that decisions shall be "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." *See also* EO 12968, Section 3.1(b) (listing multiple prerequisites for access to classified or sensitive information).

Analysis

Guideline K, Handling Protected Information

The security concern for Handling Protected Information is set out in AG ¶ 33:

> 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 evidence establishes that while Applicant was on an active duty assignment conducting threat vulnerability assessments in the Persian Gulf region in June 2004, he entered his observations in a notebook, which he kept in his travel backpack. During his downtime, he drank seven or eight alcoholic beverages at a hotel bar, where he met a Russian woman. He took her back to his hotel room, and they had consensual sex. He left her alone in his room for a brief period before they parted ways. The next day, he could not find the notebook. Although he suspected that the Russian woman took it, he did not report the loss until an interview with a polygraph examiner in January 2009.

The Government submits that Applicant violated the Secretary of the Navy Instruction (SECNAVINST) 5510.36, *Department of the Navy Information Security Program Regulation*, dated March 17, 1999, in that he failed to safeguard working papers under ¶ 7-6; did not comply with the general provisions for escorting or handcarrying classified information under ¶ 9-11; violated the storage requirements for classified information under ¶ 10-3; and did not comply with his responsibility to report the loss or compromise of classified information under ¶ 12-2. Applicant denies that he violated any of these regulations because the information in the missing notebook was not classified.

SECNAVINST 5510.36 applies to all classified national security information classified under Executive Order 12958, and predecessor orders, and special types of classified and controlled unclassified information outlined in Chapter 1 of the regulation. While personnel are individually responsible for compliance with the regulation, SECNAVINST 5510.3 does not apply to "cryptic" notes of Applicant's personal observations unless they were determined by an appropriate classifying authority to require protection against unauthorized disclosure. Applicant, as the senior CI/HUMINT analyst on his team, could be expected to know the sensitivity level of the information. In late January 2009, almost five years after the notebook was lost, he indicated to a polygraph examiner that the information was sensitive, but only when compiled in a report was it considered classified. When later asked to describe the classification level of the notebook, Applicant responded, "This information when reported is considered Secret. This information in the notebook is considered Secret." When read in context with his other statements to the effect that the notes were not classified until compiled in the report, Applicant is clearly acknowledging that the classification level of the information, when reported in his final assessment, was Secret. It does not necessarily follow that the notes of his personal observations were classified without reference to other data.

As to whether the notes themselves were classified in and of themselves without reference to other data, such as terrorist tactics, context, and digital images involved in the final assessments, the evidence is inconclusive at best. A counterintelligence professional, who performed threat vulnerability assessments with Applicant, indicates that notes were taken to assist them in completing their assessments at a later time in a classified area. He characterized such notes as "nothing more than cryptic reminders of items to address in [their] finished products." Care was taken to secure classified hardware in the field, and drafts or reports were written on computer systems under full accountability. However, notes were treated like other, non-classified personal information, and left in hotel rooms during downtime. Applicant could conceivably have entered Secret information in the lost notebook, but there is no evidence to suggest that he would have deviated from common practice.

Paragraph 7-6 of SECNAVINST 5510.36 addresses the appropriate safeguarding of classified working papers. Working papers "include classified notes from a training course or conference, research notes, drafts, and similar items that are not finished documents." If they contain classified information, they are required to be

dated when created, conspicuously marked as working paper on the first page, marked with the highest overall classification level of any information contained, protected to the level of classification assigned, and destroyed by authorized means when no longer required. (GE 6.) Applicant denies that the notebook was a working paper in that he did not obtain the information from a classified source, but rather from his own observations. Applicant's notes certainly were not finished documents, but without proof that they were classified in and of themselves, ¶ 7-6 was not violated.

Similarly, ¶ 9-11 of SECNAVINST 5510.36 requires the use of a cover sheet, file folder, or other covering to prevent inadvertent disclosure when handcarrying classified information within the command, and double-wrapping outside of the command. Applicant and his former team member in the Persian Gulf (AE D) both attest to their efforts in the field to secure classified information. There is no evidence that Applicant, while acting as their hardware courier, ever failed to secure the classified equipment in the GSA-safe that they attached to their vehicle or to a building stanchion. Nor is there any evidence that Applicant ever failed to properly prepare or secure the assessment reports, which he admits were classified. If the notebook contained classified information, then Applicant violated ¶ 9-11(b), which provides that classified information is not to be left unattended in any circumstances, and ¶ 9-11(c), "during overnight stops, classified information is to be stored at a U.S. embassy, military or appropriately cleared DoD contractor facility and shall not, under any circumstances, be stored in vehicles, hotel rooms, or safes." Yet, without proof establishing that the notebook was classified, he did not violate ¶ 9-11, or the storage requirements for classified information set forth in ¶ 10-3, "classified information not under the personal control or observation of an appropriately cleared person shall be guarded or stored in a locked GSA-approved security container, vault, or secure room."

Likewise, Applicant's failure to report the loss of the notebook, without proof that it contained classified as opposed to sensitive information, does not fall within the reporting requirements of SECNAVINST 5510.36 ¶ 12-1 and ¶ 12-2, which make it clear that a loss of classified information occurs when it cannot be physically located or accounted for, and that an individual who becomes aware that classified information is lost or compromised must immediately notify his commanding officer or security manager so that the loss can be properly investigated and actions taken to negate or minimize the adverse effects of the loss or compromise. That being said, Applicant clearly understood that he should have reported the loss of his notebook to minimize the risks of sensitive information being disclosed to unauthorized persons.

Applicant was negligent in failing to adequately protect his sensitive notes, and his failure to report the loss of that sensitive information was deliberate. Guideline K security concerns are not restricted to classified information. *See* AG ¶ 34(g), "any failure to comply with rules for the protection of classified or other sensitive information." It does not take counterintelligence training to appreciate the security risk presented by a rendezvous with a Russian woman about whom he knew little, if anything, while he was under the influence of alcohol and in a foreign locale. Applicant acknowledged at his hearing that he ran a risk "by bedding anyone down in a foreign country." (Tr. 76.)

Applicant informed the polygraph examiner in January 2009 that when preparing to go to work the morning after his rendezvous with the Russian woman, he could not find the notebook containing his observations involved in threat vulnerability assessments. He looked everywhere he could think of, but it did not turn up. It occurred to him that the Russian woman took the notebook when he was in the restroom. At his hearing, Applicant testified discrepantly that he did not realize it was lost until after he left the hotel. He was already with his team and probably at the next site, so he did not return to look for it. In either case, Applicant admitted that he should have reported the loss to a counterintelligence officer, who would have likely referred the matter to a counterintelligence division. The fact that Applicant did not report the June 2004 loss until a CI polygraph interview in January 2009 is further evidence that he knew that he had violated a command rule or practice, if not a specific regulation, concerning the proper control of sensitive information. By virtue of his TS/SCI access, Applicant had an individual responsibility to report to his cognizant security officer any activities or conduct related to the security guidelines, including foreign influence or close personal associations with foreign nationals, which could conflict with his ability to protect classified information from unauthorized disclosure or counterintelligence threats.[7]

To the extent that AG ¶ 34(g) applies, AG ¶ 35(a), "so much time has elapsed since the behavior, or it has happened so infrequently or under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or good judgment," is the only Guideline K mitigating condition possibly pertinent. Applicant handled highly classified material for most of his military career, and there is no evidence of any inappropriate handling of classified or sensitive information apart from the incident at issue. Nonetheless, his failure to report the loss of sensitive information for over four years precludes me from concluding that it happened so long ago or was so infrequent to no longer cast doubt on his reliability, trustworthiness, or good judgment. When asked to explain his failure to report the incident, Applicant responded that he was embarrassed, but also that "[he] wasn't sure that [he] had lost it either, at first, and then [he] went on to [country omitted] right afterwards." (Tr. 73.) Reform is not sufficiently demonstrated where he continues to rationalize or justify his failure to report the loss or suspected loss of sensitive information. But even if Guideline K is not firmly established because the Government

[7]*See* Annex E of the Director of Central Intelligence Directive 6/4, *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information*, dated July 2, 1998. The SOR did not allege that Applicant violated the DCID. In ISCR Case No. 03-20327 at 4 (App. Bd. Oct. 26, 2006) the Appeal Board listed five circumstances in which conduct not alleged in an SOR may be considered stating:

> (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.

Id. (citing ISCR Case No. 02-07218 at 3 (App. Bd. Mar. 15, 2004); ISCR Case No. 00-0633 at 3 (App. Bd. Oct. 24, 2003)).

failed to prove a violation of the SECNAVINST, the conduct bears negative implications for his judgment under Guideline E.

Guideline E, Personal Conduct

The security concern for Personal Conduct is set out in AG ¶ 15:

> 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.

Applicant exercised very poor judgment within AG ¶ 15 by leaving sensitive information unattended when a foreign national, about whom he knew little, had uncontrolled access. Suspecting that the foreign national had taken the notebook, Applicant chose not to report the loss because he wanted to avoid personal embarrassment, if not censure, for conduct inconsistent with the sound judgment expected of such an experienced CI/HUMINT operative. The Government established its case under 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." Furthermore, whether he was intoxicated or only "slightly buzzed," Applicant showed poor judgment in consuming seven to eight alcohol drinks and then becoming involved with a foreign national, who was essentially a stranger to him, while he was on a CI assignment for the U.S. military. When considered with his failure to timely report the loss of the notebook, AG ¶ 16(c) is also pertinent:

> (c) credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any other single guideline, but which, when considered as a whole, supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the person may not properly safeguard protected information.

As for the potentially mitigating conditions, AG ¶ 17(a), "the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts," cannot reasonably be applied, in light of Applicant's failure to report the loss of the notebook before the January 2009 polygraph. AG ¶ 17(c), "the offense is so minor, or so much time has passed, or the behavior is so infrequent, or it happened under such unique circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment," also is not pertinent. Although the Government is now aware of the lost notebook and the circumstances under which it occurred, the behavior of security

concern is not mitigated by minimizing the seriousness of his behavior (e.g., in retrospect, he would have reported the loss of the notebook "because I think that had I reported it, I would have been cleared of any wrongdoing and it would have saved me this entire process and having a problem with the polygraph."). (Tr. 77).

Applicant went on to handle highly classified information after the June 2004 incident with no violations of record. His overall record of reliability in this regard weighs in his favor. His unrebutted testimony is that he did not place himself in a potentially compromising situation with other foreign women while on duty after the incident of concern. (Tr. 95.) AG ¶ 17(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," is partially satisfied, in that he is unlikely to place himself in a similar situation in the future. That being said, his failure to report the loss of the notebook is a separate issue that continues to cast doubt on his judgment and reliability. It is difficult to reconcile his testimony that he did not think about the notebook "all that much beyond the operation" (Tr. 84) with his disclosure of the incident during the polygraph ("the notebook was the only thing that I could think of that was bad"). (Tr. 86.) To the extent that AG ¶ 17(e), "the individual has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation, or duress," is implicated because of his belated disclosure in January 2009, it is unclear whether he has been fully candid with his character references about the circumstances in which he lost the notebook in June 2004. The former chief warrant officer, who worked alongside Applicant for five months in 2002, was aware that Applicant had been administered a polygraph wherein he was questioned about a missing notebook containing his observations while performing vulnerability assessments. However, this witness did not seem to know about the circumstances of the loss of the notebook. When posed a hypothetical about social interactions with a Russian female and the immediate disappearance of a notebook containing CI notes after her departure, the witness indicated it would cause him some concern, depending on the contents of the notes. (Tr. 40.) Although Applicant has mitigated his vulnerability somewhat, it does not completely eliminate the extremely poor judgment he displayed in June 2004 and compounded by his failure to disclose the loss of the notebook for over four years.

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 his conduct and all relevant circumstances in light of the nine adjudicative process factors listed at AG ¶ 2(a).[8]

[8] The factors under AG ¶ 2(a) are as follows:

> (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

As his character references attest, Applicant was a knowledgeable CI/HUMINT professional who carried out his duties with dedication, including in various hostile environments where safeguarding classified information was a challenge. At the same time, this expertise makes it especially difficult to mitigate the poor judgment he exhibited in June 2004 while he was on a CI assignment for the U.S. military. Alcohol may well have been a significant factor in him letting down his guard with the Russian female, but it was not a factor in his failure to report the loss of the notebook. For the reasons noted above, I cannot conclude that it is clearly consistent with the national interest to allow Applicant access to classified information.

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

Subparagraph 1.a: Against Applicant

Paragraph 2, Guideline E: AGAINST APPLICANT

Subparagraph 2.a: 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 grant Applicant eligibility for a security clearance. Eligibility for access to classified information is denied.

_____
Elizabeth M. Matchinski
Administrative Judge

pressure, coercion, exploitation, or duress; and (9) the likelihood of continuation or recurrence.