KEYWORD: Security Violations; Personal Conduct

DIGEST: Applicant is a facility security officer who was held responsible by the Defense Security Service when two company employees improperly used laptop computers to process classified information at offsite locations in early 2001. Her positive discharge of her security duties over the past six years is sufficient to overcome the concerns raised by her negligence in failing to ensure compliance with computer accreditation requirements. She did not deliberately falsify her subject interviews when she denied any prior knowledge of the employees' actions. In the absence of proof that her foreign-born brothers-in-law were still foreign nationals as of her June 2005 security clearance application, her failure to list them does not raise personal conduct concerns. Clearance is granted.

CASENO: 03-06115.h1

DATE: 06/13/2007

DATE: June 13, 2007

In re:	)	
	)	
----------	)	ISCR Case No. 03-06115
SSN: ----------	)	
	)	
Applicant for Security Clearance	)	

DECISION OF ADMINISTRATIVE JUDGE
ELIZABETH M. MATCHINSKI

APPEARANCES

FOR GOVERNMENT
John B. Glendon, Esq., Department Counsel

FOR APPLICANT
Francis J. Flanagan, Esq.

SYNOPSIS

Applicant is a facility security officer who was held responsible by the Defense Security Service when two company employees improperly used laptop computers to process classified information at offsite locations in early 2001. Her positive discharge of her security duties over the past six years is sufficient to overcome the concerns raised by her negligence in failing to ensure compliance with computer accreditation requirements. She did not deliberately falsify her subject interviews when she denied any prior knowledge of the employees' actions. In the absence of proof that her foreign-born brothers-in-law were still foreign nationals as of her June 2005 security clearance application, her failure to list them does not raise personal conduct concerns. Clearance is granted.

STATEMENT OF THE CASE

The Defense Office of Hearings and Appeals (DOHA) declined to grant or continue a security clearance for Applicant. As required by Department of Defense Directive 5220.6 ¶ E3.1.2 (Jan. 2, 1992), as amended, DOHA issued a Statement of Reasons (SOR) on June 30, 2005, detailing the basis for its decision–security concerns raised under Guideline K (Security Violations) and Guideline E (Personal Conduct) of the adjudicative guidelines.[1] In a *pro se* Answer of July 20, 2005, Applicant denied the allegations with explanations and requested a hearing before a DOHA administrative judge.

On January 31, 2007, the government moved to amend the language of SOR ¶¶ 1.a, 1.b, and 1.c under Guideline K to clarify the nature of the security violations Applicant allegedly failed to report (¶¶ 1.a and 1.b) and knowingly or negligently permitted to occur (¶ 1.c) while employed as facility security officer (FSO). Under Guideline E, the government moved to amend the language of ¶¶ 2.a, 2.b, and 2.c to allege with specificity the bases for the false statements Applicant allegedly made in August 2002 (¶ 2.a), September 2002 (¶ 2.b), and January 2003 (¶ 2.c), and to add two new subparagraphs, ¶ 2.d (alleging that Applicant falsified a June 2005 security clearance application by not listing foreign relatives), and ¶ 2.e (cross-alleging the Guideline K conduct under Guideline E). The case was assigned to me on February 2, 2007, with the motion pending. On February 9, 2007, I ordered Applicant to respond by March 1, 2007, or the SOR would be amended as proposed and the allegations admitted. On February 15, 2007, Applicant indicated through counsel that she had no objections to the motion to amend.

Pursuant to notice dated February 26, 2007, I convened a hearing on April 25, 2007, to determine whether it is clearly consistent with the national interest to grant or continue a security clearance for Applicant. The SOR was amended as proposed by the government, and Applicant admitted her responsibility for the security violations in the amended SOR. The government's case consisted of 22 exhibits and the testimonies of three government investigators who interviewed Applicant and a Defense Security Service (DSS) industrial security representative. Applicant and three witnesses testified on her behalf. A transcript of the hearing was received on May 7, 2007.

[1]The SOR was issued under Applicant's married name, even though on her divorce in December 2004, she resumed use of her maiden surname (reflected above in parentheses).

FINDINGS OF FACT

DOHA alleged under Guideline K, as amended, that Applicant as FSO: (1) in or about January 2001 failed to report that a computer hard drive marked classified and a laptop circuit board for an unaccredited laptop had been used by a company employee offsite at another defense contractor's facility to process SECRET information, in violation of ¶¶ 1-200, 1-201, 1-300, 1-303, 1-304, 5-100, and Chapter 8 of the National Industrial Security Manual for Operating Information (NISPOM) and §§ III.1, III.2, and V of the company's standard practices procedures manual (SPP) (¶ 1.a)[2]; (2) in or about March and April 2001 failed to report that a computer hard drive marked classified and a laptop circuit board for an unaccredited laptop had been used to process SECRET information by a company employee at the same offsite location on two occasions in addition to that alleged in ¶1.a, in violation of ¶¶ 1-200, 1-201, 1-300, 1-303, 1-304, 5-100, and Chapter 8 of the NISPOM and §§ III.1, III.2, and V of the SPP (¶1.b); and (3) in or about March and April 2001 knowingly or negligently permitted SECRET information to be processed on two occasions on an unaccredited laptop computer system owned or under the operational control of company employees while outside of the company facility, in violation of ¶ 5-100 and Chapter 8 of the NISPOM and § X of the SPP (¶ 1.c).

DOHA alleged under Guideline E, as amended, that Applicant falsified material facts: (1) in an August 7, 2002, statement by denying she had any prior knowledge that classified information was used on unclassified computers (¶ 2.a); (2) during a September 2002 interview by denying she had any prior knowledge of the use of unclassified laptop computers to process classified information and denying she had sent out an unaccredited laptop for classified use at a defense contractor facility (¶ 2.b); (3) during a January 28, 2003, interview by denying that she had allowed or given permission for any company employee to use an unaccredited computer system to process classified information (¶ 2.c); and (4) on a June 2005 security clearance application (SF 86) by not listing her two foreign national brothers-in-law (¶ 2.d). In addition, the security violations alleged under Guideline K were cross-alleged under Guideline E (¶ 2.e).

In her Answer of July 20, 2005, Applicant explained as to ¶ 1.b that in late January 2001, she had received a package containing a hard drive and circuit board, both classified SECRET. Told they were used in a laptop owned by the Navy but operated by employees of her company at another defense contractor's facility, she indicated the Navy temporarily accredited the equipment so it could be used during a critical project pending DSS accreditation. In a supplemental response, she indicated that the hard drive and circuit board were not returned to the other company until they had been temporarily accredited by the Navy. Applicant denied knowingly or negligently permitting employees of her company to process classified information on unaccredited laptops. Applicant also denied intentional falsification of her August 2002 statement or September 2002 and January 2003 interviews with an authorized investigator. In response to the amended allegations, Applicant admitted that as FSO, she was responsible for the violations since they occurred on her watch (Tr. 11-12). After consideration of the pleadings, exhibits, and hearing transcript, I make the following findings of fact.

[2]In the original SOR, the government had alleged failure to report a security incident involving the use of an unaccredited laptop to process classified information on board submarines at a naval base in January 2001. In the amended SOR, the government focused on the alleged violations that occurred offsite at a defense contractor facility in January 2001.

Applicant is a 49-year-old FSO, who started her career as a civilian clerk-typist for the U.S. Navy in June 1976. She was first granted a SECRET clearance in late July 1976. In April 1978, she became a branch secretary for the Navy, and in July 1978 married her first husband. In August 1984, Applicant had her first child, a daughter. Two years later, she was divorced. Applicant supported herself and her daughter by working as a division/branch secretary at the naval base. As a division secretary, Applicant was in charge of the classified safes in the office.

In April 1988, Applicant married her second husband. He adopted her daughter from her first marriage, and they had two daughters who were born in November 1990 and November 1995. In June 1991, Applicant left her job at the naval base. She had been out on maternity leave and requested an additional month of unpaid leave so that she could remain with her husband, who was working for the Navy out of state and not scheduled to return until July 1991. She resigned when the leave was not granted as she could not afford to maintain a household, work full-time, and raise her two daughters on her own. After about three months unemployed, she took a position with a very small defense contracting firm. In addition to her administrative duties, she was given the job of facility security officer (FSO) responsible for personnel and facility security compliance at the workplace. Her SECRET clearance was renewed in March 1992. In early July 1995, a few months before the birth of her third daughter, she was laid off. In about February 1996, she was diagnosed with cancer, and was unable to work for about a year while undergoing treatment.

In late February 1997, Applicant returned to work. In mid-May 1997, she resumed her duties as FSO for her previous employer. She was granted a SECRET clearance in early June 1997.

In mid-April 1999, Applicant began working for her present employer (company X) in human resources and as the FSO. To fulfill her duties as FSO, Applicant had to be cleared to the level of the company's clearance.[3] The facility was cleared to the level of TOP SECRET (SECRET for storage capability) on August 15, 1996. Applicant completed a security clearance application (SF 86) on April 29, 1999. She listed her seven siblings (two brothers and five sisters) on her application (Your Relatives and Associates), but did not include two brothers-in-law who had been born in Spain. Applicant was granted her TOP SECRET clearance in mid-May 2000.

As company X's FSO, Applicant was responsible for supervising and directing the security measures necessary for implementing the Department of Defense's requirements for classified information as set forth in the NISPOM, and in the company's Standard Practices and Procedures (SPP) manual, which provided specific security guidance to cleared employees within the facility as required by NISPOM ¶¶ 1-201 and 1-202. Applicant's duties as FSO included coordinating the use of company computers for classified work and ensuring that company employees with clearances (about 130 as of August 2002) were educated about and adhered to their security responsibilities.

The DSS industrial security specialist (ISS) assigned to monitor and assist company X's security compliance visited the facility in June 2000 and found five security issues that needed correction, including some problems with the computer systems approved for classified processing.

[3]Only Applicant and the President of the company were listed as key management personnel (Owner, Officer, Director, Executive Personnel, "OODEP"). Pursuant to ¶ 2-104 of the NISPOM, the senior management official and the facility FSO must always be cleared to the level of the facility clearance. Other officials, as determined by the cognizant security authority, must be granted a personnel security clearance or excluded from classified access.

Steps were taken to have an employee with technical knowledge of computer systems adequately trained in automated information systems security. In December 2000, a non-accredited automated information system (AIS) was used to process classified information and CONFIDENTIAL information was sent unencrypted over the Internet.

On January 9, 2001, a laptop computer, which had been used by company X personnel (employee #1) to process classified information on board a Navy submarine, was sent via registered mail to Applicant's attention.[4] The package was wrapped and marked SECRET. On her receipt on January 12, 2001, she was advised by employee #1 that the package contained a laptop with hard drive that had been used by him in a classified environment. Aware it would violate security to process classified information on a company X laptop that had not been accredited by the DSS, she opened the package and asked him if it was accredited, *i.e.*, approved by DSS for processing of classified information. Applicant informed employee #1 that the laptop had to be approved ahead of time to process classified information. Employee #1 assured her that he had a technical change proposal document from the Navy that allowed the laptop to be connected to a classified system on the submarine where he was working for company X. After logging it into the classified accountability system and storing it in an approved container, she notified the DSS industrial security specialist (ISS) with cognizance over the facility.[5] The ISS advised her that if company X owned the laptop, an AIS security plan would need to be generated and accreditation requested from DSS, but that the Navy was responsible for the laptop accreditation if it belonged to the Navy.[6]

Applicant learned that the computer belonged to the Navy. She kept the laptop with hard drive in an approved GSA container at her facility until it was again needed on the submarine. On assurances from employee #1 that he had sanitized the hard drive, and on belief that an interim accreditation had been granted by the Navy for use of the laptop to process classified information on the submarine, Applicant allowed employee #1 to again use the laptop in late February 2001 to process classified information on the submarine without obtaining accreditation from DSS. She did not pursue accreditation because it was a government-owned (Navy) laptop. Applicant informed the ISS on February 26, 2001, that the laptop would be sent directly from the submarine to the Navy after its use where it would then be declassified according to Navy regulation. After the laptop was returned in its unclassified state, company X would begin the 30-day accreditation process. The ISS approved of the process proposed, and requested that once the company regained custody of the laptop, company X send in the accreditation package as well as certification of the declassification.

---

[4]The classified material transmittal document (Ex. 8) signed by Applicant on January 12, 2001, indicates that it was sent to her attention at company X. Her signature appears on the classified material transmittal document. She told a DSS polygraph examiner that employee #1 delivered the classified package to her office (Exs. 15 and 16), and that the company X employee who had used the laptop informed her of its contents before she opened it (Ex. 15). At the hearing, she testified that it brought, still wrapped, to her office by employee #1 (Tr. 150).

[5]This security incident was the subject of ¶ 1.a in the original SOR issued on June 30, 2005. DOHA amended the SOR, in part, to focus on the use of an unaccredited laptop to process classified information at the facility that was the subject of ¶ 1.b in the June 2005 SOR and now ¶1.a and ¶ 1.b. The use of the laptop on the submarine is nonetheless relevant to assessing the security posture of the facility and Applicant's knowledge of security practices as the FSO.

[6]At the hearing, the ISS testified that the DSS "generally has responsibility for such accreditation within industry. Within the Government, Government activities have their own authorization to approve certain automated information systems to process classified information." (Tr. 64).

The Navy subsequently declassified the hard drive and Applicant sent verification of that declassification to the ISS.

On January 24 and 25, 2001, a company X employee (employee #2), who was cleared to at least the SECRET level, connected an unaccredited laptop[7] to a SECRET AIS at another defense contractor facility (company Y) (SOR ¶ 1.a). Company X was a prime contractor on the contract. Employee #2 was told by a company Y employee that it was not a problem as long as the computer hard drive was treated as SECRET following the testing. At the conclusion of the classified testing, the hard drive and circuit board were removed, marked SECRET and appropriately wrapped, and sent back to company X via registered mail to the attention of employee #2. The laptop itself was hand carried. On receipt of the classified shipment on January 26, 2001, Applicant opened it and discovered it contained a laptop hard drive and circuit board, both marked SECRET. Applicant notified employee #2 of the receipt, logged both items into company X's classified accountability records, and secured them. Applicant originally thought it was test equipment and did not realize that they had been used in the laptop. The classified hard drive and circuit board were transmitted back and forth on at least two additional occasions between companies X and Y so that employee #2 and his coworkers could use them at company Y.[8] Applicant assumed they were being used properly at company Y and she did not question company X employees as to how they were being used and she did not inform the ISS.[9]

On February 16, 2001, the ISS received from Applicant an AIS security plan dealing with a laptop.[10] On March 2, 2001, the security plan was returned to company X with a number of required corrections.

On March 12, 2001, the ISS met with the Navy to ask about accreditation of the laptop used to process classified information on the submarine in January 2001. During the onsite visit, the ISS learned a second laptop had been used to process classified information by company X employees at

---

[7]There is conflicting evidence as to whether the laptop was owned by the Navy but used by company X personnel (*see* Answer) or owned by the company (*see* Ex. 15).

[8]Applicant told a DSS polygraph examiner that the hard drive and circuit board had been transferred back and forth during the March to April 2001 time frame (Ex. 16), and that she learned in May 2001 that the hard drive had been used in a laptop owned by company X for the processing of classified information (Ex. 16). She testified at her hearing that it was in late January 2001 when the hard drive came back into the facility that she investigated and determined that the laptop belonged to company X so it would have to be accredited. (Tr. 169-70)

[9]Applicant testified on direct examination that when she first received the SECRET hard drive from company Y, she assumed it was a piece of test equipment and properly stored it. (Tr. 154) The evidence is conflicting as to how and when Applicant realized the hard drive was not a piece of test equipment (*See* Tr. 160, 166-74, 188-190), but it was not shown that she ever sent out a laptop from company X to company Y knowing that it would be used to process classified information at company Y.

[10]The AIS security plan was not included in the hearing record, and it cannot be determined from the record what laptop(s) this AIS concerned. In a letter of April 17, 2001, to company X's president, the ISS indicated he received an AIS security plan pertaining to the laptop used at company Y, with no mention that the laptop had been previously used to process classified information. (Ex. 12) The inference is that Applicant sought to accredit a computer she knew had been used at company Y to process classified information, a post hoc effort at rectification. In a letter of April 10, 2001, to DISCO, the ISS indicated company X's vice president went to the Navy to obtain approval to accredit the laptop used at company Y. (Ex. 11) The vice president did not confirm that he had contacted the Navy with respect to the laptop used at company Y (Tr. 216-17), which apparently was a company and not government-owned laptop.

company Y in January 2001. Applicant was informed by the ISS in an email of March 13, 2001, that pending his completion of an administrative inquiry of the use of the two laptops, he needed the particulars of the use of the laptop at company Y (location, dates and names of employees, classified system, contract number, measures taken to protect the laptop and transmit to company X). In response on March 26, 2001, Applicant indicated that the classified hard drive had been removed from the laptop, transmitted via registered mail from company X, and stored in an approved container since it was received. A DSS investigation revealed that the laptop had been connected to an AIS approved to process SECRET information for testing on January 24 and 25, 2001, at company Y, with the classified sessions lasting six or seven hours in each instance. In an email message of March 28, 2001, the DSS representative with security cognizance over facility Y concluded that initial indications were that no compromise had occurred, but that company Y had been asked to conduct an inquiry. Company Y questioned the need for reaccreditation as the proper procedures had been followed, and it was similar to adding new workstations to the AIS which did not require reaccreditation.

On April 10, 2001, the ISS filed with DISCO an adverse information report under ¶ 1-304 of the NISPOM, assessing Applicant as responsible for two security violations involving the use of unapproved laptops to process SECRET information at company Y and on a naval submarine. The ISS indicated that Applicant had "ample knowledge of AIS security requirements through formal instruction, years of experience as well as past and present oversight of DSS accredited AIS systems." He opined that Applicant "was aware that both laptops were operating in a classified mode, left the facility on three occasions for classified use, and were returned twice as SECRET hardware. [Applicant] allowed the use of the laptops to continue, failed to stop it, or report the violations." In a letter of April 17, 2001, the ISS alerted company X's president of what he saw as the overall declining security posture at the facility. He characterized the processing of classified information on an unaccredited laptop by an employee at company Y in January 2001 as disturbing. While he could not determine the knowledge Applicant had before the processing, he indicated she should have been alerted to the problem on receipt of the marked hard drive in late January and she did not mention to him that it had been used to process classified when she submitted an AIS security plan on February 16, 2001. He commented that the recent violations demonstrated "an ongoing lack of knowledge on the part of [company X's] employees as well as [the FSO]."

Sometime in 2001, a human resource employee was hired, and Applicant assumed full-time responsibility for security at the facility. In her capacity as FSO, Applicant continued to be responsible for personnel and facility compliance with security regulations, and was the point of contact within the company for the assigned DSS representative. In January 2002, a new DSS ISS assumed security cognizance over company X.

On August 7, 2002, Applicant was interviewed by a DSS special agent about her knowledge of the use of two unaccredited laptops to process SECRET information. Applicant provided a sworn statement in which she admitted she had a detailed knowledge of the DSS standards for AIS accreditation, but she denied any prior knowledge that classified information had been processed on unclassified computers. She indicated that on receipt of the hard drive properly wrapped and shipped from company Y, she notified the employee involved that it was an unauthorized use of the computer, and contacted the DSS for advice on how to deal with the situation, that within days she had submitted security plans for company X AIS systems, and had initiated accreditation of the

computers. Applicant indicated that she had thereafter taken greater control of all computers utilized to process classified information, and provided necessary education to company X employees.

On September 3, 2002, the DSS ISS was interviewed about the administrative inquiry at company X in 2001 and the finding that no compromise had occurred. No longer the assigned DSS representative for the facility, he could not recall the actions taken to accredit the laptops at issue. He expressed his belief that Applicant did not deliberately allow the violations, but may have been somewhat incompetent with regard to the incidents.

During a subsequent interview with a DSS agent on September 5, 2002, Applicant again denied any knowledge of the use of the unclassified laptops while it was taking place, and she denied she ever sent out an unaccredited laptop from company X for classified use. She explained she had sent the hard drive back to company Y on two occasions on company Y's request but had never sent out the laptop.

On January 28, 2003, Applicant was interviewed by a DSS special agent/polygraph examiner in conjunction with a scheduled polygraph examination. During the pretest interview, Applicant denied she ever knowingly allowed or gave permission for any employee at company X to use any unclassified or unapproved (unaccredited) computer system to process classified information. Applicant explained that while the same laptop had been taken back to the submarine and used to process classified information, the Navy had provided paperwork showing the accreditation. As for the use of a second laptop at company Y, Applicant related she properly logged and stored the classified hard drive and circuit board received from company Y, and that between March and April 2001, the same classified hard drive and circuit board were transmitted back and forth between company X and company Y so that employee #2 and his cleared coworkers could use them at company Y (¶ 1.b). Applicant said she assumed the computer components were being used for processing classified information because they were both marked as classified, but she did not question anyone. Applicant indicated that she learned in May 2001 from employee #2 that the same hard drive was being used in a laptop owned by company X at company Y for the processing of classified information, and she did not allow that hard drive to return to company Y until the laptop was accredited by the DSS. During a post-test interview, Applicant acknowledged she had allowed the security violations to occur in that she made assumptions and failed to ask the required questions about the classified hard drive and circuit board. She indicated it was never her intent to allow classified information to be processed on an unapproved system and she never gave verbal permission to do so. Applicant attributed the security problems in 2001 to her being responsible for both FSO and human resource duties at that time. She denied falsifying any information during previous interviews with the ISS or DSS special agent.

To renew her TOP SECRET clearance, Applicant executed a security clearance application (SF 86) on June 27, 2005. Divorced from her second husband in December 2004, Applicant filed the application under her maiden name. Applicant listed her parents, three daughters, and seven siblings on her SF 86. While two of her brothers-in-law were foreign-born, she did not include them in response to question 9, "Your Relatives and Associates." She did not think to list them since they had lived in the U.S. for many years and are in the U.S. legally.

On June 30, 2005, DOHA issued the original SOR to Applicant under her married name. While her request for hearing was pending, Applicant was interviewed by an authorized investigator

for the Department of Defense on September 14, 2006. Asked about her foreign-born brothers-in-law, and her failure to list them on her SF 86, Applicant explained she did not realize she was required to list them on her clearance application. She was uncertain of their citizenship status, whether they had become U.S. citizens by naturalization or were citizens of their native Spain, but knew they had acquired permanent residency status in the U.S. Asked about the DSS ISS' allegations that she had known about security violations and allowed them to continue, Applicant indicated that the ISS was confusing two incidents, one that did not involve any company X personnel. Concerning the processing of classified information on board the submarine, she explained that as soon as she learned that employee #1 had used an unaccredited laptop to process classified information on the submarine, she called the ISS to determine what steps should be taken. She then discussed a second incident involving storage by company X of company Y hard drives; that in the process of investigating the classified items in company X's possession, the ISS found some of company Y's hard drives that had not been certified were found to contain classified information. (Ex. 21) It is not clear whether Applicant was discussing another security incident or the use of the laptop at company Y. Applicant denied that she made any knowingly false statements to government investigators.

As of late April 2007, Applicant was the information security officer as well as FSO for company X. An information technology professional was the information security manager with particular oversight over AIS at the facility. Continuation of Applicant's TOP SECRET security clearance is supported by upper management at the company. She has shown herself to be dependable and conscientious with regard to fulfilling her security responsibilities. Under her watch, the company has not failed any security inspections. Minor deficiencies have been corrected on the spot. Applicant has been more diligent in her efforts to acquire security expertise in the past six years.

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 occupy a position . . . that will give that person access to such information." *Id.* at 527. The President 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). An applicant "has the ultimate burden of demonstrating that it is clearly consistent with the national interest to grant or continue [her] security clearance." ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002).

The adjudicative guidelines set forth potentially disqualifying conditions (DC) and mitigating conditions (MC) under each guideline. In evaluating the security worthiness of an applicant, the administrative judge must also assess the adjudicative process factors listed in ¶ 6.3 of the Directive. The decision to deny an individual a security clearance is not necessarily a determination as to the loyalty of the applicant. *See* Exec. Or. 10865 § 7. 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.

CONCLUSIONS

Under Guideline K, noncompliance with security regulations raises doubt about an individual's trustworthiness, willingness, and ability to safeguard classified information. (Directive ¶ E2.A11.1.1). Applicant has a duty as a cleared individual to safeguard classified information under her custody or in her control (NISPOM ¶¶ 1-200, 1-500; SPP § II), and to report adverse information that comes to her attention involving any loss, compromise, or suspected compromise of classified information, or concerning any cleared (or in the process of being cleared) employee which indicates such access or determination may not clearly be consistent with the national interest (NISPOM ¶¶ 1-302a, 1-303; SPP § III.1). Furthermore, by virtue of her position as FSO, Applicant is responsible for supervising and directing security measures necessary for implementing the requirements of the NISPOM and her employer's SPP (¶ 1-201 NISPOM). Specific duties include educating employees about the government's information security program, advising them of the requirements for disclosure of classified information and contractual obligations involving classified access, informing them of the adverse impact on national security that could result from unauthorized disclosure, instructing them about the procedures for handling classified material, providing employees with the particular security requirements applicable to their jobs, alerting them about counterintelligence issues, and informing them of their reporting obligations (SPP § II.1). Any failure of an FSO to comply with security regulations necessarily raises questions about the appropriateness of continued access for the cleared facility as well as for the FSO.

Applicant did not know before January 12, 2001, that employee #1 had used an unaccredited laptop on board the naval submarine, and she acted appropriately in reporting the violation to the ISS. While the ISS subsequently concluded that Applicant violated security requirements when she permitted employee #1 to use the laptop to process classified information on the submarine a second time without first obtaining proper accreditation (Ex. 11), the evidence shows that Applicant understood from the ISS that it was the Navy's responsibility to accredit the laptop since it was owned by the government. In late February 2001, Applicant notified the ISS that the employees involved with the laptop would have it sent directly to the Navy and not company X on its return from the ship, and the laptop would be declassified according to Navy regulations before being sent back to the company. The ISS responded, "What you have described works for me." (Ex. 7) Applicant knew from her AIS training that a company X laptop had to be accredited by DSS before any classified processing. NISPOM ¶ 8-102 specifies that the cognizant security agency (DSS in the case of company X) is the designated accredited/approving authority responsible for accrediting information systems used to process classified information in industry. Yet, laptops were also new in the facility. Even DSS representatives had questions about AIS accreditation and what was required at that time (*see* Ex. 7). When questioned in September 2002 about the violations, the ISS indicated that Applicant "may have been somewhat incompetent with regard to the incidents." (Ex. 6).[11]

However, the circumstances surrounding the use of the laptop at company Y and Applicant's knowledge (what she knew and when she knew it) raise concerns under Guideline K, disqualifying condition ¶ E2.A11.1.2.2, *Violations that are deliberate or multiple or due to negligence*, and general

[11]In his letter to company X's president of April 17, 2001, the ISS indicated Applicant had "ample knowledge of AIS security requirements through formal instruction, years of experience as well as past and present oversight of DSS accredited systems." However, he also indicated that the more recent security violations involving the laptops "demonstrates an ongoing lack of knowledge on the part of [company X] employees as well as your Facility Security Officer." (Ex. 12).

concerns under Guideline E, ¶ E2.A5.1.1, *Conduct involving questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations could indicate that the person may not properly safeguard classified information*. Applicant has repeatedly maintained throughout several interviews that she did not give permission to employee #2 to process classified information at company Y on an unaccredited laptop. While Applicant told a DSS polygraph examiner in January 2003 that she had "knowingly allowed classified information to be processed on [a] computer system that was not accredited by DSS" (Ex. 14), she did not admit to prior knowledge or approval of the improper use of the laptop; rather, she admitted she failed as FSO to ensure that the hard drive and circuit board transmitted between company X and company Y were being used appropriately by company X personnel at company Y. Aware that company X employees were working on a project at company Y involving a classified circuit board and hard drive, Applicant was negligent in not inquiring into the circumstances of their use. While there is conflicting evidence as to when she confirmed with employee #2 that he had used an unaccredited company X-owned laptop, once she learned of the security violation, she had an obligation to report it to DSS under NISPOM ¶¶ 1-302.a and 1-304 and SPP § III. Although she contends she contacted DSS as soon as employee #2 confirmed he had used the unaccredited laptop, the available evidence indicates the ISS learned of the improper use of the laptop at company Y on March 12, 2001, from the Navy during his investigation of the use of the other laptop on the submarine. She did not provide any document to corroborate her claim of notification.

The success of the industrial security program within a given defense contractor facility depends on the FSO upholding his or her fiduciary duty. The demands of two positions (human resources and security) cannot justify any failure to report a known or suspected violation. However, Guideline K mitigating conditions ¶ E2.A11.1.3.2, *violations were isolated or infrequent*, and ¶ E2.A11.1.3.4, *demonstrate a positive attitude towards the discharge of security responsibilities*, apply. Due at least in part to the delay (unexplained) in the adjudication of this case, it has been six years since the laptop was used at company Y. Deficiencies in the facility's security posture between December 2000 and April 2001 have been corrected. With the hiring in 2001 of another employee to take over Applicant's human resource duties, she has been able to devote her full attention to security with positive results. The company has not failed any inspections. Minor deficiencies have been corrected on the spot. While company X's upper management has a stake in ensuring that Applicant retains her TOP SECRET clearance, the corporate officers are not likely to have falsely attested to Applicant's diligence with regard to her own security education.

Applicant's increased competency in understanding and implementing security requirements notwithstanding, the government must be assured that her representations can be relied on, and with regard to fulfilling her security responsibilities, that she will timely report any security violation or adverse information about a cleared employee that comes to her attention. Any evidence of intentional falsification would necessarily raise serious doubts about her judgment and reliability under Guideline E,[12] and about her willingness to comply with her obligations under the NISPOM, including reporting requirements. The government contends Applicant made several false statements by claiming in August 2002, September 2002, and in a pre-polygraph interview of January 2003, that she had no prior knowledge of unaccredited computers being utilized to download classified data. Submitted as

[12]*See* Directive ¶ E2.15.1.1, conduct involving questionable judgment, untrustworthiness, unreliability, lack of candor, dishonesty, or unwillingness to comply with rules and regulations could indicate that the person may not properly safeguard classified information.

proof of her falsification was Applicant's sworn statement of January 28, 2003, in which she indicated with respect to the use of the laptop at company Y:

> In about Feb 01, I received a classified package from [company Y]. . . . I opened it and saw that it contained a hard drive classified as SECRET and a circuit board classified as SECRET. . . . Between Mar 01 and Apr 01, this classified hard drive and circuit board were transmitted back and forth between [company Y and company X] so [employee #2] and his cleared coworkers could use them at the [company Y] facility. Each time they were properly wrapped and marked in keeping with DSS regulations. I assumed at the time that the hard drive and circuit board were being used properly at [company Y] so did not question anyone. I did not report this to DSS at the time, and I did not ask [company Y] officials, [employee #2] or any of our [company X] employees specifically how they were using the hard drive and circuit board.
>
> In May 01, I found out through a conversation with [employee #2] that this same classified hard drive was being used in a laptop owned by [company X] at [company Y] for the processing of classified information. At that time, I called [the ISS] and told him what happened. I did not allow that hard drive to go back to [company Y] until the [company X] laptop was accredited by DSS. By Jul 01, [company X] had this laptop and another one accredited by DSS. I now realize that by making the above assumptions and not asking all the questions about this classified hard drive and circuit board, **I did knowingly allow classified information to be processed on [a] computer system that was not approved by DSS**. . . . It was never my intent to disregard any security regulation or to commit any security violations. (Ex. 15, emphasis added).

Applicant also indicated in that same statement, "I now realize, however, that because of my title of FSO, I was responsible for the security violations because the ultimate security responsibility for my facility falls on me. I do not like the fact that I am being investigated for this security violation when it was committed by another cleared [company X] employee." (Ex. 15)

There is no evidence that Applicant knew employee #2 had used his laptop to process classified information at company Y during the week of January 22, 2001, when it was going on. Although she transmitted the circuit board and hard drive back to company Y at least twice on employee #2's request, the government did not prove that she returned a laptop with express or tacit permission to use it to process or download classified information. It was reasonable of her to assume that employee #2, who had at least a SECRET clearance, would fulfill his security responsibilities. Company Y did not see any problem with the procedure, as the equipment was logged in, and properly declassified when they finished. (Ex. 7) While this does not eliminate the need for company X to accredit the computer beforehand, it suggests that any violation of security was not deliberate but due to inadequate knowledge of security requirements. Employee #2 may not have realized that it was a violation, as employee #1 did not understand that the temporary change document was insufficient to accredit the laptop he used. Applicant's recognition, albeit in hindsight and with some reluctance, that she is responsible for the violations of employees at her facility, is not tantamount to an admission that she knew beforehand and approved of the improper use of a laptop. Based on the

evidence before me, I conclude Applicant did not deliberately falsify her statement and interviews as alleged in ¶¶ 2.a, 2.b, and 2.c.

Nor did the government prove a knowing falsification of her June 2005 security clearance application. Applicant does not dispute that she failed to list on her June 2005 SF 86 the two brothers-in-law who were born in Spain. The government bases its case for Guideline E DC ¶ E2.A5.1.2.2, *The deliberate omission, concealment, or falsification of relevant and material facts on any personnel security questionnaire, personal history statement, or similar form used to conduct investigations, determine employment qualifications, award benefits or status, determine security clearance eligibility or trustworthiness, or award fiduciary responsibilities*, solely on the fact of foreign birth of these two relatives. Assuming the instructions for completing the EPSQ version of the SF 86 (Ex. 20) are the same as the Questionnaire for National Security Positions (Ex. 22), Applicant would have been required to report those "foreign national" relatives or associates to whom she is bound by affection, obligation, or close and continuing contact. Applicant readily admitted to an investigator in September 2006 that two of her sisters are married to former professional Jai-Alai players born in Spain. However, she also indicated that she was not certain whether her brothers-in-law were still citizens of Spain or had become U.S. citizens by naturalization. Their citizenship status was not sufficiently clarified at the hearing to permit the threshold finding that they were foreign nationals as of her execution of the June 2005 security clearance application. If they acquired U.S. citizenship and did not possess dual citizenship, they would not be foreign nationals as a matter of law.

FORMAL FINDINGS

The following are my conclusions as to each allegation in the SOR, as amended:

Paragraph 1. Guideline K:	FOR APPLICANT
Subparagraph 1.a:	For Applicant
Subparagraph 1.b:	For Applicant
Subparagraph 1.c:	For Applicant
Paragraph 2. Guideline E:	FOR APPLICANT
Subparagraph 2.a:	For Applicant
Subparagraph 2.b:	For Applicant
Subparagraph 2.c:	For Applicant
Subparagraph 2.d:	For Applicant
Subparagraph 2.e:	For Applicant

DECISION

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

Elizabeth M. Matchinski
Administrative Judge